NACHA Third-Party Sender Certification Program Criteria

INTRODUCTION

These Third-Party Sender Certification Program Criteria set forth the subject matter areas that will be reviewed by NACHA in order to determine whether an applicant ("Applicant") satisfies NACHA's requirements to become a certified Third-Party Sender ("TPS") within the ACH network. NACHA's assessment of an Applicant's compliance or a certified TPS' on-going compliance with each of the criteria below will be made in NACHA's sole discretion. NACHA may revisit such assessment at any time, may at any time request a TPS to provide additional information to support its ongoing certification, and may revoke a certification based on changes to underlying facts or changes to the standards applied by NACHA for evaluating the sufficiency of an Applicant's or TPS' qualifications. NACHA may designate third parties to assist in the conduct of any on-site review or other aspect of the certification process.

PART A: INITIAL APPLICATION FOR TPS CERTIFICATION

The following criteria apply to the initial application ("Application") to become a certified TPS.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
1.0 Business Duration		
Applicant must have been in business at least two (2) years at the time the Application is submitted.		Applicant to certify the date on which Applicant was established.
2.0 Fees		
(A) Applicant must pay the non-refundable application fee specified by NACHA from time to time (B) If NACHA incurs extraordinary expenses in order to complete the certification process for Applicant, including travel expenses relating to onsite reviews, NACHA may require Applicant to reimburse NACHA for such costs		Payment of Fee and, as applicable, costs.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
3.0 Background of Applicant		
Applicant and each relevant individual must (A) give NACHA authorization to perform criminal background checks on Applicant and (i) each Principal of Applicant and, if Applicant is a subsidiary of another company, each Principal of Applicant's ultimate holding company, and (ii) each Key Officer or (B) attest and provide evidence as requested by NACHA that the entity has been cleared through all applicable background checks for all state licenses required by that entity. The results of such background checks must be acceptable to NACHA. For these purposes, a "Principal" is each individual who owns 25% or more of the equity interest of Applicant or its ultimate holding company, and the "Key Officers" are Applicant's Chief Executive Officer, Chief Financial Officer, Chief Compliance Officer, Chief Operating Officer and Chief Risk Officer, or the equivalent.		(1) Applicant and each relevant individual to provide authorization in a form established by NACHA from time to time, and (2) background checks completed with results acceptable to NACHA.
4.0 Financial Condition		
Applicant must provide specified financial documentation, which NACHA will review to assess the topics listed below to confirm to NACHA's satisfaction that Applicant has the financial stability and wherewithal to fulfill its obligations as a Third-Party Sender.		Applicant must provide NACHA with copies of Applicant's (i) two most recent audited annual financial statements and (ii) most recent quarterly financial statement. If Applicant is a subsidiary of another company, Applicant also must provide copies of such audited

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
The information provided by Applicant will be reviewed by NACHA to assess the following: (A) Whether Applicant has a minimum net worth of $250,000; (B) The soundness of Applicant's financial condition; (C) Applicant's solvency; (D) The adequacy of Applicant's capital relative the expected volume of ACH activity and the level or risk associated with Applicant's Customers;[1] and (E) The adequacy of Applicant's reserves and controls in place to (i) access and control Customer funds, (ii) delay settlement to support investigation of Customers, (iii) offset its loss exposure from origination, and (iv) meet its obligations regarding the timing and processing of funds to Customer accounts.		financial statements for its ultimate parent holding company. If Applicant does not have audited financial statements separate from those of its parent company, Applicant must provide unaudited financial statements together with an attestation of accuracy and a copy of the parent company audited financial statements.
5.0 NACHA Rules Compliance		
(A) General Rules Compliance Applicant must demonstrate compliance with the NACHA Operating Rules.	NACHA Operating Rules 1.2.2	Applicant must provide NACHA with a completed copy of its most recent NACHA Rules Audit demonstrating compliance with the NACHA Operating Rules.

[1] An Applicant's Customers include the Applicant's Originators, and any other Third-Party Sender (each a "Nested Third Party") for which the Applicant originates.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
		If Applicant has not had a completed NACHA Rules Audit within the 12 month period prior to submission of the Application, it must complete a NACHA Rules Audit and submit the results to NACHA before NACHA acts on the Application; provided that if Applicant has been providing payment processing services in connection with payment card network transactions for at least [two] years prior to the date of the application, NACHA will consider the application subject to (1) Applicant's providing NACHA with such additional information as NACHA may request in its discretion regarding such activities, and (2) Applicant agreeing to have a NACHA Rules Audit conducted promptly after engaging in Third-Party Sender activities for one year and providing such NACHA Rules Audit to NACHA upon its completion. If the applicable NACHA Rules Audit shows any noncompliance or other exceptions to the NACHA Operating Rules, Applicant must provide NACHA with documentation demonstrating the steps that Applicant has taken (or will take) to correct such noncompliance and exceptions.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
(B) Compliance with Requirements Relating to ACH Origination Agreements		
(i) Generally Applicant must have an executed Origination Agreement in place for each Customer for which it originates ACH entries that complies with the requirements for Origination Agreements set forth in the NACHA Rules.	• NACHA Operating Rule 2.2.2	To the extent compliance is not adequately addressed in the NACHA Rules Audit provided pursuant to Section 5.0(A) above, NACHA may request that Applicant (i) provide a certification by a Senior Official that Applicant meets the criterion and/or (ii) provide NACHA with a copy of Applicant's current sample Origination Agreement and policy/procedure for ensuring that Origination Agreements are executed for each Customer for which Applicant originates. If the NACHA Rules Audit demonstrates, or NACHA otherwise is advised by Applicant, that Applicant has Origination Agreements in place with Applicant's customers that vary substantially from Applicant's sample Origination Agreement, NACHA may require Applicant to provide further information regarding Applicant's customer Origination Agreements that vary in material respects from the sample Origination Agreement.
(ii) Specific Requirements for ACH Origination Agreements Applicant's Origination Agreements must contain the following terms, which may not varied by agreement between Applicant and the Customer:	• NACHA Operating Rule 2.2.2 and best practices	See comments for Section 5.0(B)(i) above. In addition, at NACHA's request, Applicant must provide an explanation of triggers and processes by which Applicant can lower ACH limits or otherwise restrict ACH transactions for a Customer.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following

• Agreement to be bound by the NACHA Operating Rules.
• Agreement not to originate Entries that violate the laws of the United States.
• Any restrictions on the types of Entries that may be originated.
• Termination provisions including the right of Applicant to terminate the Agreement for cause, including, but not limited to cause for (a) violation of applicable laws, rules, regulations or other regulatory requirements ("Applicable Law") or the NACHA Rules, (b) fraudulent or otherwise illegal activity and (c) excessive returns.
• Right of audit provisions giving Applicant the right to audit Customers to ensure compliance with the NACHA Rules and the Agreement.
• Applicant's Origination Agreements should also address, without limitation:
  ○ Terms under which the Customer will be required to pre-fund ACH transactions or provide other financial comfort
  ○ Terms under which the Customer must notify Applicant of material changes in financial status or other changes that would affect Applicant's risk analysis and underwriting process for customer		

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
6.0 Compliance and Risk Program		
Introduction: NACHA's primary approach to an Applicant's Compliance and Risk Program is to rely on Applicant's certification and confirm that Applicant's Compliance and Risk Program includes appropriate policies, procedures, and internal controls, and that Applicant is performing in accordance with such policies, procedures, and internal controls. In the event that NACHA determines, in its discretion, to review any of Applicant's policies, procedures, internal controls, or other documentation relating to its Compliance and Risk Program, NACHA's review may also encompass an assessment of the appropriateness and effectiveness of such policies, procedures, internal controls and other documentation.		
Applicant must have adopted and implemented, and be performing in accordance with, a "Compliance and Risk Program" that includes, without limitation, policies, procedures and internal controls relating to, at a minimum, risks associated with the following topics addressed in subsections of this Section 6.0: • General compliance with Applicable Laws (see subsection (A) of this Section 6.0); • Compliance with know your customer ("KYC") and know your customer's customer ("KYCC") requirements (see subsection (B) of this Section 6.0); • Compliance with anti-money laundering ("AML") and Office of Foreign Assets Control ("OFAC") requirements (see subsection (C) of this Section 6.0); • Information security compliance (see subsection (D) of this Section 6.0); and • General risk management (see subsection (E) of this Section 6.0).		a. Applicant must provide a certification by Applicant's president, CEO, Chief Compliance Officer, Chief Risk Officer or other senior official acceptable to NACHA ("Senior Official") that (i) Applicant has adopted and implemented a Compliance and Risk Program that meets the applicable criteria for this Section 6.0, (ii) Applicant is performing in accordance with its Compliance and Risk Program and (iii) the Compliance and Risk Program and Applicant's implementation and performance thereof satisfies Applicant's obligations under federal and state laws and regulations, including, but not limited to, as a vendor to insured depository institutions. b. Upon NACHA's request, Applicant will make available for review by NACHA Applicant's policies, procedures, internal controls, risk assessments and other documentation relating to Applicant's Compliance and Risk Program

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
In addition, Applicant must perform ACH Risk Assessments as described in subsection (F) of this Section 6.0.		
If Applicant processes for a Nested Third Party: • Applicant shall be responsible for requiring the Nested Third Party to satisfy Third-Party Sender Certification Program Criteria to the same extent as Applicant itself. However, no such Nested Third Party shall be considered a Certified Third-Party Sender, or hold itself out as such, unless it independently applies and is approved for certification by NACHA; and • Applicant must have adequate contractual protection, policies, procedures and controls to enable it to mandate and oversee performance by any Nested Third Party to the same standards as Applicant's own performance.		c. Upon NACHA's request, Applicant will make available to NACHA evidence of any Nested Third Party's satisfaction of these criteria
6.0(A) General Legal Compliance		
(i) Compliance with Federal and State Laws Generally Applicant's Compliance and Risk Program must include a program for (a) determining the Applicable Laws that govern Applicant's activities, and (b) undertaking compliance with such Applicable Laws.	• Applicable Laws governing Applicant's operations, products and services • FFIEC Third-Party Risk Management Guidance • NACHA Operating Guidelines, Chapter 2	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
(ii) Compliance with Federal/State Registration/Licensing Requirements Applicant must have all registrations and licenses required under federal and/or state law, as applicable.	• FinCEN Money Services Business registration requirements • State money transmitter laws • State consumer lending laws	
6.0(B) KYC and KYCC Compliance		
Applicant's Compliance and Risk Program must include a structured and repeatable KYC and KYCC program designed to identify, validate, and provide information regarding each Customer, and, if Applicant processes for a Nested Third Party, each Originator for which such Nested Third Party processes. The program must require Applicant to identify each such entity and each Principal of each such entity. Applicant's Compliance and Risk Program must include a process to respond to ODFI inquiries about transactions and to provide a complete listing of the following within 24 hours of any request from its ODFI(s): • All Originators Applicant services. • All Nested Third Parties with whom Applicant does business and their underlying Originators. Applicant's Compliance and Risk Program must include policies and procedures to ensure that no Nested Third Party that is a	• BSA/AML rules and guidance (including such provisions contained in 31 CFR Chapter X) • OFAC Requirements • FFIEC Third-Party Risk Management Guidance	In addition to the certification required under Section 6.0, if Applicant processes for Nested Third Parties, a Senior Official must certify that no Nested Third Party for which Applicant processes itself performs processing for other Third-Party Senders. At NACHA's request, Applicant shall make available Applicant's polices and procedures and/or customer Origination Agreement language precluding a Nested Third Party customer from processing for another Third-Party Sender.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
customer of Applicant processes for any other Third-Party Sender.		
6.0(C) AML and OFAC Compliance		
Applicant's Compliance and Risk Program must include the development, adoption and implementation of a documented OFAC and AML program that includes at least the following elements. With regard to OFAC compliance, Applicant must screen all of its Customers (and screen, or ensure that its Nested Third Parties screen, all Originators of its Nested Third Parties) against all sanctions lists administered by OFAC, including without limitation the Specially Designated Nationals (SDN) List, and report any matches as required by OFAC regulations and block transactions as required. With regard to AML compliance, Applicant must develop, implement and maintain an effective anti-money laundering program ("AML Program"). An effective AML Program is one that is reasonably designed to prevent Applicant from being used to facilitate money laundering and the financing of terrorist activities. Applicant's AML Program, at a minimum, must comply with Applicable Law and regardless of whether Applicant is required to maintain an AML Program under	• NACHA Operating Guidelines, Chapter 3	Applicant shall make copies of the AML Program available for inspection by NACHA upon request.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
Applicable Law, must meet the following criteria: • The AML Program shall be commensurate with the risks posed by the location and size of, and the nature and volume of the ACH services provided by, Applicant. • The AML Program shall be in writing. • The AML Program must, at a minimum: ○ Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with the criteria in this Section and with any Applicable Law governing Applicant's AML activities. ○ Include and implement policies, procedures, and internal controls for complying with the following: ▪ verifying the identity of Customers and their Principals, consistent with industry best practices for customer due diligence; ▪ identifying money laundering activities, financing of terrorist		

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
activities, or other suspicious activities and reporting them to appropriate authorities; ▪ creating and retaining records; and ▪ responding to law enforcement requests. • The AML Program must include a process to screen Nested Third Parties. • The AML Program must require that Applicant's Nested Third Parties also have a process to screen the Nested Third Party's Originators. • The AML Program must include a requirement to screen all Customers for which it processes and all Originators of Nested Third Parties, for negative media. • The AML Program must designate a person to assure day to day compliance with the AML Program. • The AML Program must provide require Applicant to conduct an AML risk assessment at least annually, document the results of such risk assessment and any identified risk mitigation steps,		

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
including the implementation of changes necessary to maintain an effective AML Program. • The AML Program must include education and/or training of appropriate personnel regarding their responsibilities under the Program, including the detection of suspicious transactions. • Applicant must conduct an independent review (using internal or external resources) to monitor and maintain the AML Program with a scope and frequency that is commensurate with the risks posed by Applicant's ACH activities.		
6.0(D) Information Security Compliance		
Applicant's Compliance and Risk Program must include a documented information security program that is designed to identify, address, and mitigate known and emerging threats and vulnerabilities ("Information Security Program"). Applicant's Information Security Program must, at a minimum, address the topics described in subsections (i) through (vii) of this Section 6.0(D).	• FFIEC Cybersecurity Assessment Tool • Gramm-Leach-Bliley Act (GLBA) – Interagency Guidelines Establishing Information Security Standards (12 CFR 30, App. B (OCC); 12 CFR 208, App. D-2 and 12 CFR 225, App. F (Fed); 12 CFR Part 364, App. B (FDIC) / 12 CFR 748 (NCUA) / FTC Safeguards Rule (16 CFR 314.3, 314.4) • State Data Security Laws • NACHA Operating Rules 1.6	
(i) The Information Security Program must (a) require Applicant to perform	• FFIEC Cybersecurity Assessment Tool	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
vulnerability and penetration testing at least quarterly, on a schedule determined based on risk factors, and take effective and sustainable corrective actions to address deficiencies discovered during testing, and (b) provide that at least annually such tests are conducted through an independent third party.		
(ii) The Information Security Program must include the implementation of appropriate administrative, technical, and physical safeguards to protect ACH account data.	• GLBA – Interagency Guidelines Establishing Information Security Standards/FTC Safeguards Rule • State Data Security Laws • UDAP – Section 5 of FTC Act (15 USC 45(a)/Dodd-Frank Act (12 USC 5531) • NACHA Operating Rules 1.6	
(iii) The Information Security Program must include the implementation of policies and procedures that are designed to protect and secure ACH account data from unauthorized access from both internal and external sources.	• NACHA Operating Rules 1.6	
(iv) The Information Security Program must require Applicant to encrypt, or transmit via a secured session, banking and financial account information related to an ACH Entry at all times from the point of data entry through transmission of such banking and financial account	• NACHA Operating Rules 1.7	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
information, using technology that provides a commercially reasonable level of security that complies with Applicable Laws (with exceptions for transmissions by means of voice or keypad inputs from a wireline or wireless telephone to a live operator or Voice Response Unit (VRU)).		
(v) The Information Security Program must require Applicant to provide a written report on the overall status of the information security and business continuity programs to its Board or an appropriate Board committee (or comparable bodies) at least annually.	• FFIEC Cybersecurity Assessment Tool.	
(vi) The Information Security Program must include a process for threat information sharing with other industry participants to enhance Applicant's preparedness for, and ability to prevent, security incidents.	• FFIEC Cybersecurity Assessment Tool.	
(vii) The Information Security Program must (a) provide for an independent audit or review of Applicant on at least an annual basis to evaluate policies, procedures, and controls across Applicant's business for significant risks and control issues related to information security, and (b) require that the independent audit or	• NACHA Operating Rules 8.2(g)	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
review must be in the form of and SSAE 16 SOC 1 or SSAE 16 SOC 2 audit, or similar auditing standards for the financial services industry.		
6.0(E) General Risk Management		
(i) Risk Management Program		
Applicant's Compliance and Risk Program must include a documented risk management program with clearly defined objectives and clearly defined risk parameters ("Risk Management Program"), including, but not limited to, compliance risks, credit risks, operational risks, and reputational risks. The Risk Management Program must include an ongoing process that evaluates whether ACH activities are conducted within the risk parameters set out in the program and whether or not existing controls, processes and policies effectively address all aspects of ACH origination. At a minimum, the Risk Management Program must address the topics described in subsections a and b of this Section 6.0(E)(i), and the topics addressed in subsections 6.0(E)(ii) through (vii) below. a. The Risk Management Program must (i) outline how and how often Applicant is providing reporting of results against parameters (for example, monthly metrics reported by Applicant in comparison to risk	• OCC Bulletin 2006-39, *ACH Activities* • FFIEC Third-Party Risk Management Guidance	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
parameters), and (ii) include a process for corrective action for exceptions to approved risk tolerances.		
b. Applicant must maintain a list of prohibited lines of business, prohibited types of Originators, whether direct or through a Nested Third Party, and restricted geographies, and must comply with such prohibited lists.	• OCC Bulletin 2006-39, *ACH Activities*	
(ii) Risk Management Systems and Controls: Underwriting and Creditworthiness		
a. The Risk Management Program must include a formal Approve/Decline policy (approval process).	• OCC Bulletin 2006-39, *ACH Activities*	
b. The Risk Management Program must include adequate credit risk program controls that establish formal underwriting standards, require analysis of each Customer's creditworthiness, set appropriate credit exposure limits, and evaluate the financial condition, including capital strength and operating income, of any Nested Third Party for which Applicant processes.	• OCC Bulletin 2006-39, *ACH Activities*	
c. The Risk Management Program must include policies governing processes for establishing	• NACHA Operating Rules 2.2.3 and 2.15.3	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
ACH credit and debit dollar exposure limits for Customers, including compliance with SEC Code-specific entry authorization requirements.		
d. The Risk Management Program must include documented underwriting standards that include, at a minimum: • a background check of each Customer and their Principals and negative file inquiry in credit reporting databases • a list of permissible SEC ACH entry types • verification that the Customer is operating a legitimate business • a review of any generally available negative reports and/or customer complaint reports (e.g. Better Business Bureau complaints, complaints on websites such as RipoffReport.com) • a review of any state or federal regulatory and law enforcement actions		
e. The Risk Management Program must require Applicant to perform due diligence on each Customer sufficient to form a reasonable belief that the Customer has the capacity to perform its obligations in compliance with the NACHA Rules.	• NACHA Operating Rules 2.2.3 and 2.15	
f. The Risk Management Program must require Applicant to maintain credit files on each of its Customers that include the types of		

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
transactions that are authorized, Applicant's analysis and evaluation of the Customer's creditworthiness, and approved Exposure Limits.		
g. The Risk Management Program must provide for an annual review by Applicant of each Customer's financial condition to ensure it has not changed.		
h. Risk Management Program must include established credit and debit Exposure Limits for Customers.	• NACHA Operating Rules 2.2.3, 2.15	
i. The Risk Management Program must require Applicant to periodically assess the nature of each Customer's ACH activity and the risk it presents.	• NACHA Operating Rules 2.2.3 and 2.15	
j. The Risk Management Program must include procedures to enforce restrictions on the types of Entries that may be originated. k. If Applicant processes for a Nested Third Party, the Nested Third Party must comply with Applicant's Risk Management Program with respect to the Nested Third Party's Originators.	• NACHA Operating Rules 2.2.3 and 2.15	
(iii) Risk Management Systems and Controls: Monitoring		

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
a. The Risk Management Program must require Applicant to monitor compliance with Customers' Exposure Limits across multiple Settlement Dates.	• NACHA Operating Rules 2.2.3	
b. The Risk Management Program must include adequate controls to monitor Customer activity in accordance with industry best practice, including, at a minimum: • periodic account review; • ongoing activity monitoring; • exceptions; • suspect activity investigations; • consumer complaints about Customers; • ODFI or RDFI complaints about Customers; • enforcement actions or law enforcement investigations against Customers; and • loss control.		If Applicant processes payments for customers in other payment channels, including, but not limited to, credit/ debit/ stored value cards, wires, or Remotely Created Checks (RCCs), Applicant must provide NACHA with a list of those additional payment channels, and the average return/chargeback/disputed item rates by payment channel, including ACH, for the most recent 12-month period.
c. The Risk Management Program must (i) include adequate policies to enable Applicant to identify and research underlying facts and circumstances when it is originating for any Customer (or any Originator of a Nested Third Party) for which Applicant has processed at least 500 ACH entries over any consecutive 60 day period or any consecutive two calendar month period, if such Customer (or any Originator of a Nested Third Party) had an Unauthorized Return Rate of over 0.5%; (ii) include tools to monitor	• NACHA Operating Rules 2.17.2.1-.3; 8.113	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
Unauthorized Return Rates to ensure acceptable levels and thresholds; and (iii) include a process to document historical issues and provide evidence on how issues were researched and resolved.		
d. The Risk Management Program must include adequate policies to enable Applicant to flag and research underlying facts and circumstances for any Customer (or any Originator of a Nested Third Party) for which Applicant has processed at least 500 ACH entries over any consecutive 60 day period or any consecutive two calendar month period, if such Customer (or any Originator of a Nested Third Party) had an Administrative Return Rate of greater than 3% during such period.	• NACHA Operating Rules 2.17.2.4-.6; 8.6	
e. The Risk Management Program must include adequate policies and processes to enable Applicant to flag and research underlying facts and circumstances for any Customer (or any Originator of a Nested Third Party) for which Applicant has processed at least 500 ACH entries over any consecutive 60 day period or any consecutive two calendar month period, if such Customer (or any Originator of a Nested Third Party) had an Overall Return Rate of greater than 15% for such period and to inquire as to the nature of the returns.	• NACHA Operating Rules 2.17.2.4-.6; 8.71	

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
(iv) Risk Management: Reporting The Risk Management Program must require Applicant to produce and review operational and management reports as needed to maintain the safety and security of ACH operations.		
(v) Risk Management: Settlement The Risk Management Program must include adequate controls and reserves to enable Applicant to meet its ACH payment system obligations, including: • Access to and control of Customer funds • Delayed settlement controls to support investigations of Customers • Adequacy of reserves or other financial protections to offset potential loss exposure from origination • Timing and processing of funds to Customer accounts • Reserve amounts adjusted for any settlement risk assumed by Applicant by making funds available to the Customer prior to final settlement through the ACH network		
(vi) Risk Management: Risk Assessment The Risk Management Program must provide for an annual review and audit of Applicant's Compliance and Risk Program, of a scope that		

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
is appropriate based on the size and type of operations of Applicant.		
(vii) Risk Management: Exceptions The Risk Management Program must include clearly documented processes for identifying, reporting, investigating and escalating complaints and exceptions, including generating reports with a documented resolution for each complaint. The processes must include the reporting to the ODFI of any sanctions issues (doing business with OFAC blocked parties) and suspicious account activity (BSA/AML). The Risk Management Program must include a process for monitoring for exceptions to processing limits, and approval levels for exceptions.		
6.0(F) ACH Risk Assessment		
Applicant must perform a risk assessment with a frequency commensurate with growth and changes in Applicant's ACH program and evolving risks in the market. Third-Party Sender	NACHA Operating Rules 1.2.4, 2.15	Applicant must provide NACHA with a copy of its most recent ACH risk assessment, which must be current within the immediate preceding 12 months. If Applicant has not performed an ACH risk assessment within the 12 month period prior to submission of the Application, it must promptly complete an ACH risk assessment and submit the results to NACHA before NACHA acts on the Application.
7.0 Return Rates		
Applicant must comply with the return rate requirements of the NACHA Operating Rules	NACHA Operating Rules 2.17	Applicant must provide NACHA with such information as NACHA may request from time to time concerning Applicant's return rates for the

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
		12-month period prior to the date on which the Application is submitted In addition to the certification required under Section 6.0, a Senior Official must certify that no Customer of Applicant has exceeded an Unauthorized Return Rate of 0.5%, an Administrative Return Rate of 3% or an Overall Return Rate of 15% for more than three months in the past 12-month rolling period. If Applicant is unable to provide this certification, it must identify each Customer that has exceeded the applicable Return Rate and describe the steps that Applicant is taking to reduce the Return Rate for such Customer to acceptable levels.
8.0 Additional Criteria		
8.0(A) Business Resiliency		
Applicant must have a documented disaster recovery and business continuity plan ("BCP Plan") that is appropriate to the size and complexity of Applicant's business and consistent with its overall business strategy. Applicant must implement its BCP Plan in the even of a disaster or other event covered by the BCP Plan. The BCP Plan must, at a minimum, comply with or address the topics described in subsections (i) through (iv) of this Section 8.0(A).	• FFIEC Business Continuity Planning Booklet • FFIEC Cybersecurity Assessment Tool (Cybersecurity Maturity, Domain 5) • FFIEC Information Security Booklet • SSAE 16/SOC 1/SOC 2 auditing standards	At NACHA's election, Applicant will provide an attestation by a Senior Official that Applicant meets these criteria and/or access to a copy of Applicant's Disaster Recovery and Business Continuity Plans.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
(i) The BCP Plan must specify the timeframe to resume activities and recover data, and integrates consideration of cyber incidents. (ii) The BCP Plan must be independently reviewed and approved at least annually. (iii) The BCP Plan must require that (a) the BCP Plan is tested on an enterprise-wide basis at least annually; (b) any issues identified as a result of such testing are remediated and the outcome of such remediation steps are documented; (c) the testing program is reviewed on a regular basis; and (d) the BCP Plan is updated on a continual basis to reflect changes in Applicant's operating environment. (iv) The BCP Plan must include training of employees that is designed to ensure that they are aware of their roles in the implementation of the BCP Plan.		
8.0(B) Insurance		
Applicant must have insurance coverage commensurate with the level of risk of Applicant's operations. This may include hazard or fidelity bond coverage, cyber liability or cyber risk insurance, or other insurance, as appropriate.		Applicant to provide proof of insurance coverage. *(NOTE: Proof of insurance coverage may be a factor in NACHA assessment of financial viability if the underlying business activities pose inherent risk of financial loss.)*

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
9.0 Optional Criteria		
The criteria in this Section 9.0 will be considered in NACHA's discretion on a case by case basis		
9.0(A) Training and Education Programs		
(i) Applicant must have a training program designed to provide employees and independent contractors effective relevant training, including training on amendments to the NACHA Rules, at least annually to remain current in knowledge and skills. Courses may include those licensed to provide continuing education credit for Accredited ACH Professional ("AAP") program.		Applicant must provide a written statement evidencing annual training, including: • Title/description of each course attended • Number of total hours of training provided by each course attended • List of employees successfully completing each course Applicant also must provide information regarding testing, certification, or other metrics used to gauge employee learning, in addition to confirming attendance.
(ii) Applicant must have qualified staff responsible for ACH operations, including AAP certified staff.	• NACHA AAP Certification Standards	Applicant must provide a list of AAP certified staff (to be checked against internal NACHA records).
9.0(B) Corporate Governance and Management		
(i) Applicant's management/leadership personnel must have sufficient relevant experience and expertise.		Applicant to provide, at NACHA's request, biographies, and tenure of all Key Officers, including explicit statements of their relevant experience to their current positions. Background checks (including criminal background checks) on Key Officers.
(ii) Applicant must have an acceptable turnover rate in Key Officer positions and the following positions:		Applicant must provide metrics showing turnover rate in past three years for stated positions.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
• General Counsel/Chief Legal Officer • Chief Privacy Officer (CPO) • Chief Information Security Officer (CISO) • Head of BSA/AML function		* If Applicant has been in operation for less than three years, Applicant will provide metrics showing turnover rate since Applicant began operations.
(iii) Applicant must not have an unacceptable level of litigation or regulatory or law enforcement actions regarding Applicant or its Key Persons, whether or not related to any aspect of Applicant's business.		Applicant must provide information regarding any pending or past litigation, regulatory or law enforcement actions against Applicant or any Key Person, or an attestation by a Senior Official that there are no such actions.
9.0(C) Reputation Risk		
Applicant must have a reputation in the industry and community that is acceptable to NACHA, and not have any red flags indicating potential fraudulent or illegal activity or other risks or concerns.	• FFIEC Third-Party Risk Management Guidance	NACHA will review by conducting an open source research to evaluate Applicant's history of consumer complaints and any negative media coverage. NACHA may request additional records of Applicant performance, including records of customer complaints

PART B: TPS OBLIGATIONS ONE YEAR AFTER RECEIVING TPS CERTIFICATION

The following criteria apply to an entity (a "TPS") that was certified by NACHA as a Third-Party Sender.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
1.0 Financial Condition		
The TPS must demonstrate continued financial stability as described in Part A, Section 4.0.		The TPS must provide NACHA with copies of the TPS' (I) most recent audited annual financial statement (unless the most recent statement was provided with the Initial Application) and (ii) most recent quarterly financial statement.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
		If the TPS is a subsidiary of another company, the TPS also must provide copies of such audited financial statements for its ultimate parent holding company. If the TPS does not have audited financial statements separate from those of its parent company, the TPS must provide unaudited financial statements together with an attestation of accuracy and a copy of the parent company audited financial statements.
2.0 Compliance and Risk Program		
The TPS must demonstrate the continued effectiveness of its Compliance and Risk Program. Note: NACHA's primary approach to an Applicant's Compliance and Risk Program is to rely on Applicant's attestation described in the column to the right. In the event that NACHA determines, in its discretion, to review any of Applicant's policies, procedures, internal controls, or other documentation relating to Applicant's Compliance and Risk Program, NACHA's review may also encompass an assessment of the appropriateness and effectiveness of such policies, procedures, internal controls and other documentation.		(i) <u>Attestation</u>. The TPS must provide an attestation by a Senior Official that the TPS has not experienced (i) a material increase in any return rate, (ii) a material violation, or allegation of a material violation, of law, regulations or the NACHA Rules, (iii) a material change in the aggregate risk profile of TPS' Originators, including without limitation an increase in processing volume for high risk Originators or the filing of claims of fraudulent or unlawful conduct against TPS' Originators, (iv) a material increase in the entries processed for other third-party senders, including the commencement of processing for third-party senders for the first time, (v) a

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
		material increase in suspicious activity in connection with transactions processed by TPS, or (vi) a breach of TPS' data security. For purposes of this paragraph, "TPS' Originators" refers to Originators whose Origination Agreements are either with TPS or a third-party sender processed by TPS. If the TPS cannot provide this attestation without qualification, the TPS must provide NACHA with a detailed written description of each material change in risk (including return rates), or violation of law, regulations or NACHA Operating Rules associated with the TPS' activities as an exception to the attestation. (ii) Onsite Review. Upon NACHA's request, the TPS will make available for review by NACHA the TPS' policies, procedures, internal controls, risk assessments and other documentation relating to the TPS' Compliance and Risk Program
3.0 NACHA Rules Compliance		
The TPS must demonstrate continued compliance with the NACHA Operating Rules.	NACHA Operating Rules 1.2.2	The TPS must complete a new NACHA Rules Audit within the prior 12 month period and submit a copy of the report to NACHA.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
		If the TPS was a provider of payment processing services in connection with payment card network transactions and did not provide a NACHA Rules Audit at the time its Application was submitted (see Part A, Section 5.0(A) above), after engaging in Third-Party Sender activities for one year following its certification, the TPS must promptly complete a NACHA Rules Audit and provide the results to NACHA. If the new NACHA Rules Audit shows any noncompliance or other exceptions to the NACHA Operating Rules, the TPS must provide NACHA with documentation demonstrating the steps that the TPS Applicant has taken (or will take) to correct such noncompliance and exceptions.

PART C: TPS OBLIGATIONS TWO YEARS AFTER RECEIVING TPS CERTIFICATION

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
1.0 Financial Condition		
The TPS must demonstrate continued financial stability as described in Part A, Section 4.0.		The TPS must provide NACHA with copies of the TPS' (i) most recent audited annual financial statement (unless the most recent statement was provided with the Initial Application) and (ii) most recent quarterly financial statement. If the TPS is a subsidiary of another company, the TPS also must provide copies of such audited financial statements for its ultimate parent holding company. If the TPS does not have audited financial statements separate from those of its parent company, the TPS must provide unaudited financial statements together with an attestation of accuracy and a copy of the parent company audited financial statements.
2.0 Compliance and Risk Program		
The TPS must demonstrate the continued effectiveness of its Compliance and Risk Program. Note: NACHA's primary approach to an Applicant's Compliance and Risk Program is to rely on Applicant's attestation and certification described in the column to the right. In the event that NACHA determines, in its discretion, to review any of Applicant's		The TPS must provide each of the following: (i) <u>Attestation</u>. The TPS must provide an attestation by a Senior Official that the TPS has not experienced (i) a material increase in any return rate, (ii) a material violation, or

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
policies, procedures, internal controls, or other documentation relating to Applicant's Compliance and Risk Program, NACHA's review may also encompass an assessment of the appropriateness and effectiveness of such policies, procedures, internal controls and other documentation.		allegation of a material violation, of law, regulations or the NACHA Rules, (iii) a material change in the aggregate risk profile of TPS' Originators, including without limitation an increase in processing volume for high risk Originators or the filing of claims of fraudulent or unlawful conduct against TPS' Originators, (iv) a material increase in the entries processed for other third-party senders, including the commencement of processing for third-party senders for the first time, (v) a material increase in suspicious activity in connection with transactions processed by TPS, or (vi) a breach of TPS' data security. For purposes of this paragraph, "TPS' Originators" refers to Originators whose Origination Agreements are either with TPS or a third-party sender processed by TPS. If the TPS cannot provide this attestation without qualification, the TPS must provide NACHA with a detailed written description of each material change in risk (including return rates), or violation of law, regulations or NACHA Operating Rules associated with the TPS' activities as an exception to the attestation. (ii) Certification.

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
		The TPS must provide a certification by a Senior Official that (a) the TPS has adopted and implemented a Compliance and Risk Program that meets the applicable criteria set forth in Part A, Section 6.0, (b) Applicant is performing in accordance with its Compliance and Risk Program and (c) the Compliance and Risk Program and the TPS' implementation thereof satisfies the TPS' obligations under federal and state laws and regulations, including, but not limited to, as a vendor to insured depository institutions. (iii) Onsite Review. Upon NACHA's request, the TPS will make available for review by NACHA the TPS' policies, procedures, internal controls, risk assessments and other documentation relating to the TPS' Compliance and Risk Program
3.0 NACHA Rules Compliance		
The TPS must demonstrate continued compliance with the NACHA Operating Rules.	NACHA Operating Rules 1.2.2	The TPS must complete a new NACHA Rules Audit within the prior 12 month period and submit a copy of the report to NACHA. If the new NACHA Rules Audit shows any noncompliance or other exceptions to the NACHA Operating Rules, the TPS must provide NACHA with documentation demonstrating the

Criteria	Source/References	Proving Compliance: Applicant to Provide the Following
		steps that the TPS Applicant has taken (or will take) to correct such noncompliance and exceptions.
4.0 ACH Risk Assessment		
The TPS must demonstrate to NACHA's satisfaction that the TPS' third party sender activities will not present an unacceptable level of risk.		The TPS must provide NACHA with a copy of its most recent ACH risk assessment, which must be current within the immediate preceding 12 months.
5.0 Additional Background Checks		
Applicant and each relevant individual must give NACHA authorization to perform criminal background checks on each Principal and Key Officer of the TPS that joined the TPS following the initial TPS certification.		(1) Applicant and each relevant individual to provide authorization using in a form established by NACHA from time to time, to perform criminal background checks on each Principal and Key Officer of the TPS that joined the TPS following the initial TPS certification, and (2) background checks completed with results acceptable to NACHA.
6.0 Fees		
(A) The TPS must pay the non-refundable certification renewal fee specified by NACHA from time to time (B) If NACHA incurs extraordinary expenses in order to complete the process of renewing the TPS' certification, including travel expenses relating to onsite reviews, NACHA may require the TPS to reimburse NACHA for such costs		Payment of Fee and, as applicable, costs.

NOTES AND LIST OF GUIDANCE

SELF-REPORTING OBLIGATIONS:

Each TPS will have an ongoing self-reporting obligation to provide written notice of the following to NACHA within 30 days of the TPS becoming aware of the applicable event:

- Any material adverse finding in any internal or external compliance, risk management or financial audit;
- Any of the TPS' Customers, or Originators of Nested Third Parties, exceeding the Unauthorized Entry Return Rate Threshold, the Administrative Return Rate Level or the Overall Return Rate Level, or
- Any material failure of the TPS to comply with Applicable Law or regulations, the NACHA Rules or the TPS' Compliance and Risk Program.

Each notice that describes a material issue will include the TPS' plan for curing the issue, including the timelines for completing such cure.

ACH-RELATED GUIDANCE:

- OCC Bulletin 2006-39, *Automated Clearing House Activities* (Sept. 1, 2006), https://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html

FFIEC IT-RELATED GUIDANCE:

- FFIEC Cybersecurity Assessment Tool, https://www.ffiec.gov/cyberassessmenttool.htm
- FFIEC IT Handbook, http://ithandbook.ffiec.gov/it-booklets.aspx
- FFIEC Business Continuity Planning Booklet, http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

FFIEC THIRD-PARTY RISK MANAGEMENT GUIDANCE:

- Federal Reserve SR 13-19/CA 13-21, *Guidance on Managing Outsourcing Risk* (Dec. 5, 2013) https://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm
- OCC Bulletin OCC 2013-29, *Third-Party Relationships* (Oct. 30, 2013) http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
- CFPBS Bulletin 2012-03, *Service Providers* (Apr. 13, 2012) http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf

- FDIC FIL 44-2208, *Managing Third-Party Risk* (June 6, 2008) http://www.fdic.gov/news/news/financial/2008/fil08044a.html
- NCUA Letter to Credit Unions 07-CU-13, *Evaluating Third Party Relationships* (Dec. 2007) http://www.ncua.gov/Resources/Documents/LCU2007-13.pdf
- FFIEC IT Booklet, *Outsourcing Technology Services*, http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx