OPERATING PROCEDURES

Version 1.0

These Operating Procedures specify the procedures, policies, and guidelines applicable to the eCheck.Net Service provided by Authorize.Net Corp. ("**Authorize.Net**") on behalf of any participating merchant (the "**Merchant**") pursuant to the eCheck.Net Service Agreement (the "**Agreement**") between the Merchant and Authorize.Net. The Operating Procedures also contain general informational regarding electronic checks and differences from other types of payment methods.

All Merchants should carefully review these Operating Procedures to understand their rights and responsibilities in using the eCheck.Net Service. Failure to strictly adhere to these Operating Procedures may result in the suspension or termination of the eCheck.Net Service by Authorize.Net as provided in the Agreement. Authorize.Net reserves the right to amend or modify the terms of these Operating Procedures at any time as provided in the Agreement. In the event Authorize.Net makes a material amendment or change, Authorize.Net will (a) notify Merchants of any material amendments or modifications, (b) update the version number for the Operating Procedures, and (c) post the new version in the Messages section of the Authorize.Net merchant account interface, which can be accessed by going to <www.authorize.net> and using the required login ID and password, or such other location specified by Authorize.Net. The amendment or modification will be effective ten (10) days from such posting.

I. Introduction

The eCheck.Net Service offers an innovative method of electronic payment for merchants and their customers in a web-based environment. Traditionally, Merchants operating on the Internet were limited to acceptance of credit cards and snail-mailed paper checks as methods of payment for their goods or services. In contrast, "eCheck.Net Transactions" include any electronic check, debit or credit or batch settlement completed or submitted by Merchants to Authorize.Net using the eCheck.Net Service for transactions involving the sale of good and services by Merchants to their customer (the "**Purchaser**").

Specifically, the eCheck.Net Service utilizes the Automated Clearing House ("ACH") to facilitate fund transfers between Merchant and Purchaser bank accounts. In addition to the terms of the Agreement, the service and all eCheck.Net Transactions are governed by the requirements of the National Automated Clearing House Association ("NACHA") Operating Rules, the Electronic Fund Transfer Act (15 U.S.C. 1693 et seq.), and Regulation E (12 C.F.R. Part 205), as promulgated by the Federal Reserve Board. eCheck.Net Transactions are ACH transactions under these regulations and laws. These Operating Procedures describe some of the legal and regulatory requirements, as well as those required by Authorize.Net, applicable to the eCheck.Net Service.

eCheck.Net Transactions between Merchants and Purchasers operate in the same manner as direct deposit paychecks between employers and employees and electronic mortgage payments between homeowners and their mortgage companies. Thus, the eCheck.Net Service enables millions of potential customers, who either lack use of a credit card or prefer to fund purchases directly from their bank accounts, to make online purchases from participating merchants. Key features and requirements of the eCheck.Net Service include:

- The eCheck.Net Service is only available to Merchants that are: (1) U.S.-based corporations, Limited Liability Companies (LLCs) or Limited Liability Partnerships (LLPs), (2) foreign corporations that do business in the United States and only use the eCheck.Net Service for U.S. consumers and with U.S. banks, or (3) U.S. Citizens or Residents, who are at least 18 years old and have been issued a social security number (SSN). Merchants must hold and maintain a bank account in the United States with a U.S.-based financial institution.
- The eCheck.Net Service processes transactions only in U.S. dollars.
- eCheck.Net enables Merchants to obtain payment from a Purchaser via direct debit to the Purchaser's bank account.
- eCheck.Net Transactions are not processed in real-time and do involve more risk for a Merchant than credit card transactions.

- eCheck.Net Transactions are not guaranteed and can be revoked by the Purchaser without the protections present with card transactions. Among other things, such revocations may result in debits being reversed and charged to the Merchant, called "Chargebacks."
- Authorize.Net acts as the "Originator" of eCheck.Net Transactions and sets processing volume and transaction amount limitations for each Merchant.
- All eCheck.Net Transactions must be authorized by the Purchaser. The Purchaser's authorization must be in writing, signed or "similarly authenticated." The similarly authenticated standard is discussed in detail in Section VI below.
- On average, eCheck.Net Transaction amounts are paid to the Merchant approximately seven (7) calendar days after submission to Authorize.Net. The length of the holding period varies among Merchants, based on Authorize.Net's internal underwriting guidelines and determination of the potential account risk for each Merchant.
- eCheck.Net Transactions will appear on a Merchant's customer's bank statement as "ECHECK TRANSACTION XXXXXXXXXX" where the Xs represent a 10 character abbreviation of the Merchant's business name.

II. Overview of the eCheck.Net Transaction Process

When initiating eCheck.Net Transactions, Purchasers provide Merchants with their bank account number and their financial institution's nine-digit routing number, both of which are found on the bottom of their paper checks. This information can be given to the Merchant verbally, in written format, or by electronic means over the Internet. Regardless of who keys the information into the Authorize.Net Virtual Terminal payment form (Purchaser or Merchant), the information is encrypted and sent securely over the Internet to Authorize.Net payment servers. Following is a list of the steps required to initiate and complete an eCheck.Net Transaction:

1. Merchant submits an eCheck.Net Transaction to Authorize.Net for processing.
2. Authorize.Net credits Merchant's virtual eCheck.Net ACH processing account for the amount of the eCheck.Net Transaction.
3. Authorize.Net initiates an ACH debit to the Purchaser's bank account the following business day; and the Purchaser's bank account is usually debited within 1-2 business days thereafter.
4. If the requested funds are available for debit from the Purchaser's bank account, they are forwarded to Authorize.Net by Purchaser's bank through the ACH system.
5. If the requested funds are not available for debit from the Purchaser's bank account, the original debit is posted back to the Merchant's virtual eCheck.Net ACH processing account as a "Returned Item". Reasons why an ACH debit might be returned include, but are not limited to, insufficient funds, invalid account or routing number, account closed, or account frozen. The amount of each Returned Item, along with a Returned Item Fee, is posted as a debit to the Merchant's virtual eCheck.Net ACH processing account by Authorize.Net.
6. On average, eCheck.Net Transactions submitted to Authorize.Net are considered "collected" by Authorize.Net if, by the seventh (7^{th}) calendar day following the settlement date of the original debit from the Purchaser's bank account, the debit has not been returned by the Purchaser's financial institution. The length of the holding period varies among Merchants, based on Authorize.Net's internal underwriting guidelines and determination of the potential account risk for each Merchant.
7. Authorize.Net transfers "collected" funds from Merchant's virtual eCheck.Net ACH processing account to Merchant's checking account every business day. All payments are subject to set-off for fees and other amounts owed by the Merchant to Authorize.Net.
8. Even though Authorize.Net transfers "collected" funds to Merchant's bank account, there still exists a small chance (due primarily to regional variances in speed and efficiency of financial institutions) that a Returned Item may be processed after the Authorize.Net-established waiting period.
9. The possibility remains that Authorize.Net will have transferred collected ACH funds to a Merchant's checking account, only to have a Purchaser instruct its bank to process an ACH reversal for reasons such as cancellation of order, non-receipt of goods or services purchased, or fraud. These reversals, called "Chargebacks," are discussed in further detail in Section IV.

III. General Limitations on Use of the eCheck.Net Service

A. Merchant Status

The eCheck.Net Service is only available to Merchants that are: (1) U.S.-based corporations, Limited Liability Companies (LLCs) or Limited Liability Partnerships (LLPs), (2) foreign corporations that do business in the United States and only use the eCheck.Net Service for U.S. consumers and with U.S. banks, or (3) U.S. citizens or Residents, who are at least 18 years old and have been issued a SSN. Merchants also must hold and maintain a bank account in the United States with a U.S.-based financial institution. The eCheck.Net Service processes transactions only in U.S. dollars.

B. Single Merchant Account

A Merchant's use of the eCheck.Net Service shall be restricted to a single merchant acquiring bank account. Merchants shall not submit payment data to Authorize.Net or otherwise process orders on behalf of any other entity or individual. Any attempt by a Merchant to use the eCheck.Net Service for more than one merchant acquiring bank account or on behalf of another entity or individual may result in an obligation to pay to Authorize.Net additional fees and charges and/or Authorize.Net's revocation of Merchant's right to use the eCheck.Net Service and termination of the Agreement.

C. Presentation of ACH Debit Requests to Authorize.Net

Merchant must present each ACH debit request to Authorize.Net within one (1) business day after the date of the transaction between Purchaser and Merchant. Merchant may not present directly or indirectly to Authorize.Net any ACH debit request that was not originated as a result of a transaction between a Purchaser and Merchant.

D. Recurring Transactions

If Merchant uses the eCheck.Net Service to accept transactions from a Purchaser that occur on a periodic basis for the purchase of goods or services that are delivered or performed periodically by Merchant to or for a Purchaser (each a "**Recurring Transaction**"), Merchant shall require the Purchaser to complete and deliver to Merchant a request for the periodic debit from the Purchaser's account and authorization that includes (1) the amount of the Recurring Transaction, (2) the account and routing number of the bank account to which the recurring debit will be submitted, (3) the frequency of charge, (4) the duration of time for which Purchaser's permission is granted, and (5) language indicating that the Purchaser may revoke the authorization by notifying the Merchant in the manner specified in the authorization. An example of a Purchaser's authorization for a Recurring Transaction is attached as Exhibit A.

In addition, Merchant shall also (i) retain the Purchaser's written authorization for the Recurring Transaction(s) for the duration of the recurring charges and provide a copy of such authorization to Purchaser, upon request; (ii) not complete an initial or subsequent Recurring Transaction after receiving a cancellation notice from a Purchaser; and (iii) require a Purchaser that elects to renew a Recurring Transaction to complete and deliver to Merchant a request and authorization for the renewal of such Recurring Transaction.

E. ACH Credit Transactions

Merchant may use the eCheck.Net Service to process ACH credit transactions only for Purchasers previously debited by Merchant through Authorize.Net's payment gateway. In no event shall the amount of any credit transaction submitted to Authorize.Net be greater than the amount originally debited from Purchaser's checking account by Merchant through Authorize.Net's payment gateway.

F. Not Sufficient Funds

Authorize.Net **does not** re-submit debits returned from a Purchaser's bank due to Not Sufficient Funds (NSF). The merchant, however, may re-submit the item to Authorize.Net and, to the extent permitted by law, may mark up the amount of the re-submitted debit to cover the amount of the applicable eCheck.Net Returned Item Fee charged by Authorize.Net. Merchants must clearly post notice to their customers informing them that NSF debits will be re-submitted with an additional returned payment fee added to the original debit amount.

G. No Guarantee of Payment; Risk of Loss

ACH payments are not guaranteed nor are they processed in real-time. Merchants bear the entire risk of loss if an ACH debit is rejected or reversed. Because it takes a certain number of days, determined by Authorize.Net in its sole discretion, from the submission of the eCheck.Net Transaction to Authorize.Net for funds to be considered "collected" by Authorize.Net, Merchants should wait at least the same amount of time before shipping or giving access to merchandise purchased by use of the eCheck.Net Service. Merchants should be mindful of the fact that the

benefits they accrue by accepting ACH transactions, i.e., ease of use and convenience, can be outweighed by the costs of accepting ACH transactions, namely due to increased risk via repudiation of the transaction.

H. Settlement with Merchant

Settlement of eCheck.Net Transactions occurs every business day, excluding bank holidays. eCheck.Net Transactions submitted to Authorize.Net before the settlement cutoff of Noon Mountain Time are sent to the bank that same day, and the time at which the batch of transactions settles becomes the time from which the applicable Authorize.Net waiting period begins. The eCheck.Net Service automatically calculates, down to the second, the time at which transactions are considered collected and available for transfer to a Merchant's bank account. Transfer of collected funds to the Merchant's bank account occurs only on business days following the time the transactions are considered collected by the system. Collected funds that show transferred on any given day will not actually be available at their financial institution until the next business day.

I. Bank Statements

eCheck.Net Transactions will appear on a Purchaser's bank statement as "ECHECK TRANSACTION XXXXXXXXXX" where the Xs represent a 10-character abbreviation of the Merchant's business name that is chosen by the Merchant during the eCheck.Net application process. Merchants should properly disclose and notify their customers that their electronic check transaction will be listed on their bank statement as "ECHECK TRANSACTION XXXXXXXXXX" to help prevent Purchasers from unnecessarily initiating a Chargeback due to the uncertainty of the source of the transaction.

IV. Chargebacks

Authorize.Net acts as the "Originator" of the transaction on behalf of the Merchant. An Originator is a person or entity that has authorized a financial institution, such as a bank, to transmit a credit or debit entry to the deposit account of a Purchaser. Therefore, from a financial institution's point of view, the only parties to an eCheck.Net Transaction are Authorize.Net and the Purchaser whose bank account is being debited. The importance of this issue comes into full view when considering the impact of chargeback transactions to both the Merchant and Authorize.Net, as explained below.

Even though an eCheck.Net debit transaction may have successfully withdrawn funds from a Purchaser's bank account, federal law and banking regulations grant a sixty (60) calendar day window (beginning from the date the financial institution first made available to the Purchaser its bank statement with the applicable debit transaction listed on it) during which a Purchaser may return any electronic ACH debit item erroneously posted to the Purchaser's bank account. To return an erroneously posted ACH debit, a Purchaser must sign a notarized affidavit at its financial institution stating that neither the Purchaser, nor any other authorized signatory on the Purchaser's account, authorized the ACH debit in question. If the affidavit is signed within the 60-day window, the Purchaser's financial institution returns the ACH debit to Authorize.Net (the Originator of the debit transaction), who in turn posts the returned item to the merchant's virtual eCheck.Net ACH processing account. Authorize.Net refers to this type of returned item as a Chargeback and accordingly posts a Chargeback Fee to the Merchant's virtual eCheck.Net ACH processing account.

Merchants typically will have sufficient funds in their virtual eCheck.Net ACH processing account to cover the amount of any Returned Item Fees and Chargeback Fees when they are incurred. If sufficient funds do not exist in a Merchant's virtual eCheck.Net ACH processing account, however, Authorize.Net initiates an ACH debit to the Merchant's bank account or charges the Merchant's credit card for the amount by which the Merchant's eCheck.Net ACH processing account is overdrawn.

A. Differences Between eCheck.Net and Paper Check Debit Transactions

eCheck.Net debit transactions are different from conventional paper check transactions, most notably with regard to the concept of repudiation. After a paper check is signed and issued by a checking account holder, the check writer (Purchaser) can only stop payment on a check before the check is presented for payment to the checking account holder's financial institution. After the check is successfully presented for payment to the issuing financial institution, the check writer loses all ability to cancel or otherwise repudiate the paper check transaction against the merchant that accepted and cashed the check (however, the check writer may make claims against the issuing financial institution for an unauthorized check). This mechanism ensures the finality of payment from a paper check. Merchants might erroneously assume similar finality of payment from electronic ACH debit transactions. With proper debit authorization procedures in place, a Merchant does have legal grounds to require payment from a Purchaser through other means, but once an ACH debit transaction (e.g., an eCheck.Net Transaction) is returned by a bank for reasons classified as a Chargeback, the Merchant cannot initiate another electronic ACH debit transaction

to the Purchaser's bank account for the same eCheck.Net Transaction. A Merchant's recourse is limited to requesting payment by some other means from the Purchaser or commencing legal proceedings to force payment.

B. Differences Between eCheck.Net and Credit Card Transactions

eCheck.Net debit transactions also differ from credit card transactions with respect to chargeback rights and procedures. In a credit card transaction, if a cardholder questions or otherwise disputes a transaction posted to the cardholder's account, the cardholder can require proof from a merchant that the cardholder authorized the transaction. Once such a request is initiated, the merchant is notified and asked to provide proof that the cardholder authorized the transaction in question. For card-present transactions, merchants either swipe or obtain a manual imprint of the card and then require the purchaser to physically sign a slip authorizing the transaction. Presentment of the signed slip, assuming a valid signature, substantiates a merchant's claim that the merchant was authorized to process the card transaction and usually protects the merchant from the risk of chargeback loss.

In the virtual world, however, Internet-based credit card transactions are, by definition, classified as card-not-present and protection from chargeback loss is only afforded by the same mechanisms used by Merchants engaged in mail/telephone order (MOTO) transactions, namely: proof of positive Address Verification Service (AVS) response and signed proof of delivery of goods to the address providing a positive AVS match. Positive AVS response, visual verification that the signature on the card matches the signature on the sales slip and visual verification that the name on the card matches that shown on some form of Government ID are all tools that exist to protect the merchant from fraudulent chargeback claims in the card world. These tools, however, are not available for eCheck.Net Transactions, neither is the opportunity available for a Merchant to refute a Purchaser initiated ACH Chargeback as it might with a credit card transaction.

C. Precautions to Reduce the Likelihood of a Chargeback

Additional precautions should be taken by Merchants to minimize the risk of loss incurred while utilizing the eCheck.Net Service for two distinct reasons. First, there is no automatic way to verify that an account number provided by a Purchaser is valid, short of personally calling the Purchaser's bank and verifying that the Purchaser does indeed have an account in good standing. Second, no mediation process exists to resolve disputes between Purchaser and Merchant. In the event an eCheck.Net Transaction is returned as a Chargeback, a Merchant's recourse is limited to requesting payment by some other means from the Purchaser or commencing legal proceedings against the Purchaser to force payment.

Such precautions include adopting a fraud transaction detection system as discussed in Section V. Further, to reduce the likelihood of a Chargeback, the Merchant may consider not shipping goods until eCheck.Net Transaction amounts are deposited into Merchant's bank account after the required Authorize.Net holding period.

V. Internet-Initiated ACH Transactions -- "WEB" Transactions

NACHA has adopted specific rules that apply to Internet-initiated entries for ACH debit or credit transfers, called a "WEB" entry. Effective January 1, 2002, the rules were promulgated as a result of three considerations: (1) the anonymity of the Internet creates an environment in which parties are not certain with whom they are doing business thereby increasing the risk of fraud, (2) the Internet is an open network which requires special security procedures, and (3) the sheer number and speed with which payments can be transacted over the Internet. This section describes the NACHA obligations of Merchants using the eCheck.Net Service for Internet transactions. More information on NACHA rules and requirements can be found at <www.nacha.org>. Each Merchant needs to make its own commercially reasonable decisions on how to implement the NACHA obligations.

A WEB entry is a debit entry to a "Consumer Account" initiated by the Merchant pursuant to an authorization received over the Internet. A Consumer Account is an account held by a financial institution and established by a natural person primarily for personal, family or household purposes and not for commercial purposes. Therefore, Internet-initiated business-to-business transactions are excluded though Merchants are encouraged to nevertheless implement the security and risk management principles applicable to WEB transactions. Any authorization that was received in person, through the mail or over the telephone is not considered a WEB transaction and the requirements of this section do not apply.

A. Commercially Reasonable

For WEB transactions, Merchants are required to ensure that certain aspects of the transaction have been addressed in a commercially reasonable manner. A "commercially reasonable" system, technology, practice or process is one that corresponds to commonly accepted commercial practices among commonly situated Merchants that conduct similar types of transactions. In other words, a Merchant should act in a way that a similarly situated merchant would have under the facts and circumstances. To determine whether a Merchant has used commercially reasonable

efforts, the analysis would include a weighing of the cost to the Merchant against the resulting benefit. The standard will change inherently as technology and the industry changes over time so Merchants must stay current and make adjustments. NACHA requires Merchants to use commercially reasonable efforts to meet the following requirements.

1. Employ a Fraudulent Transaction Detection System to Screen Each Entry

The choice of which particular fraudulent transaction detection system is appropriate for a Merchant is generally a decision for the Merchant in view of the nature of its business, product and service offerings, and customer relationships. One of the best ways of reducing the potential for fraud is to implement a transaction system that is capable of authenticating the identity of a Purchaser. For instance, Merchants can establish accounts with customers once authenticated and issue passwords and PINs for online transactions. These type of identity credentials should not be issued until the customer has sufficiently been identified such as through a credit check or review of identification. Therefore, it is important for Merchants to be able to distinguish between new and existing customers.

Systems that track payment history as well as purchasing behavior and type also should be used along with sufficient authentication to further reduce the risk of fraud. For example, a Merchant can monitor those account numbers that have resulted in a returned transaction, such as a Chargeback. A Merchant can also monitor the transaction amount, the type of goods or services purchased, the type of customer (new or existing), and the method of delivery to evaluate those transactions that may pose a higher risk of fraud. No matter what system the Merchant elects to use, some system must be used.

To help Merchants implement a fraud protection system, Authorize.Net has contracted with iShopSecure, Inc. to offer the TRANSACT-SECURE™. iShopSecure's patent pending server-based solution prevents Purchaser identification fraud by allowing a Merchant to automatically perform real-time multi-tiered authentication of the Purchaser's identity during checkout. Fraudsters are prevented from committing credit card and eCheck.Net fraud during checkout, and Purchasers are prevented from committing "friendly fraud" by later denying their own transactions. For more information about the TRANSACT-SECURE™ service, Merchants should refer to the Authorize.Net website at <www.authorizenet.com/support/transact-secure.php>.

2. Establish a Secure Internet Session with Each Purchaser

A secure Internet session should be established prior to and during the key entry by the Purchaser of the banking information utilizing a commercially reasonable security technology providing a level of security that, at a minimum, is equivalent to 128-bit encryption technology. Establishing such a connection is relatively simple and available technology through Authorize.Net. The eCheck.Net Service automatically establishes a 128-bit Secure Sockets Layer (SSL) connection with a Purchaser's browser to process an eCheck.Net Transaction.

Merchants should take care to use a secure server to collect account information from its customers online. Merchants should also consider (a) using a secure session when collecting other forms of personally identifying information (such as names, phone numbers, social security numbers, etc.), (b) publishing a FAQ or other information about using a secure browser to properly inform consumers, and (c) using a timeout feature for secure connections to avoid other users of a shared computer from accessing account or transaction information.

3. Verify that Routing Numbers Associated with Purchasers' Accounts are Valid

Verifying bank routing numbers is important to reduce administrative returns that frequently result from consumers entering wrong information or information that is otherwise not valid for their account. The use of bad routing numbers can be reduced through a variety of methods. First, the Merchant can maintain a list of administrative returns from prior transactions so that those routing numbers are not accepted in the future. Routing numbers can also be checked against commercially available databases. Second, properly informing consumers is recommended. Merchants should post clear messages to consumers regarding the accounts that they can use for ACH transactions. Demand deposit accounts and standard checking accounts may be used for ACH transactions but savings or money market accounts frequently may not. Further, the user interface should clearly explain the location and form of a routing number (such as a visual image of a check with indicators) to assist consumers in properly identifying the number. Merchants should consider using an interface that does not permit the entry of anything other than nine digits.

Authorize.Net is in the process of developing an online system to work with the eCheck.Net Service to validate routing numbers. This validation service is expected to be implemented in the first quarter of 2002.

B. Other Requirements

In addition, NACHA requires that Merchants who accept WEB transactions must conduct audits at least once a year to ensure that Purchaser financial information is protected by security practices and procedures. Such practices and procedures should ensure that the financial information collected by the Merchant from its Purchasers is protected by adequate levels of (1) physical security to protect against theft, tampering, or damage; (2) personnel and access controls to protect against unauthorized access and use, and (3) network security (such as using encryption) to ensure secure capture, storage and distribution of financial information.

Merchants can meet this audit requirement in several ways. It can be a component of a comprehensive internal or external audit, or it can be an independent audit or security seal program that covers the enumerated points above. To assist Merchants in self-evaluating their systems, a checklist of items to be evaluated in an audit are attached as Exhibit C. As the Originator of ACH transactions on behalf of Merchants, Authorize.Net conducts its own comprehensive security audits to evaluate its systems and procedures for compliance with these requirements.

VI. Authorization Requirements

In accordance with Regulation E and the NACHA Operating Rules, Merchants must obtain proper authorization from the Purchaser before initiation of ACH debit or credit entries to the Purchaser's bank account at any financial institution. All authorizations must be (1) displayed in writing to the Purchaser and (2) signed or "similarly authenticated" by the Purchaser.

A. Writing Requirement for Electronic Authorizations

For single, in person point of sale ("POS") or WEB transactions to meet the requirement that an authorization be displayed in writing to the Purchaser, an electronic authorization must (1) be able to be displayed on a computer screen or other visual display that permits the Purchaser to read it, (2) be readily identifiable as an authorization, and (3) clearly and conspicuously state its terms including the dollar amount, the effective date of the transfer, and whether the authorization is for a one-time purchase or for a recurring transaction. For any recurring transaction, the authorization must provide that the Purchaser may revoke the authorization only by notifying the Merchant in the manner specified in the authorization.

At this time, a proper authorization must consist of the following elements:

- Written language readily identifiable as an authorization by the Purchaser to the transaction (i.e., "I authorize Merchant to debit my account.")
- Clear and conspicuous statement of the terms of the transaction, including amount
- The date the authorization was granted and the effective date of the transaction (the date before which the debit transaction may not be processed).
- The account number to be debited.
- The name and nine-digit ABA/Routing number of the Purchaser's financial institution.
- For Recurring Transactions, written language indicating that the Purchaser may revoke the authorization by notifying the Merchant in the manner specified in the authorization.

B. Signature or "Similarly Authenticated" Requirement

A Merchant can always satisfy the writing and signature requirement by requiring its Purchasers to submit an ACH authorization card, an example of which is attached as Exhibit B. However, any authentication mechanism that provides assurance similar to a paper-based signature satisfies this "similarly authenticated" standard. The "similarly authenticated" standard permits signed, written authorizations to be provided electronically, such as through electronic signatures. The writing and signature requirements further are satisfied by compliance with the Electronic Signatures in Global and National Commerce Act (commonly referred to as "E-SIGN", 15 U.S.C. §§ 7001 *et seq.*), which defines electronic signatures and electronic records. Under E-SIGN, an "electronic signature" is an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. An electronic record is a record, such a contract, created, generated, sent, communicated, received, or stored by electronic means. Examples of electronic signatures include, but are not limited to, digital signatures, security codes, shared secrets, and PINs.

To satisfy this standard, the authorization process must evidence (1) the Purchaser's identity (i.e., "authenticate" the Purchaser) and (2) his or her assent to the authorization. The authorization and the authentication of that authorization must occur simultaneously. It is not acceptable to have identified a Purchaser at the time of logging on to a website and then later consider that log-in an authentication for purposes of authorizing an ACH debit. It is also

not acceptable to authenticate an authorization simply by a "click-through" process such as having a Purchaser merely press an "I Agree" button.

C. Authentication Considerations

For Merchants conducting WEB transactions, authenticating a specific Purchaser poses significant difficulties and risk. The most important component of a Merchant's fraudulent transaction system for WEB transactions is authentication of the Purchaser. "Know Your Customer" procedures are paramount to reducing fraud. Merchants are ultimately responsible for authenticating Purchasers and establishing appropriate anti-fraud systems. Given that Merchants are financially responsible for unauthorized transactions or fraudulent transactions (in the form of reversals such as Returned Items and Chargebacks), it is each Merchant's interest to adopt adequate levels of authentication.

For instance as discussed above, a fraud prevention system should distinguish between new and existing customers and establish different procedures for authenticating them and their payment and purchasing behavior. Given that there is no uniform standard for authenticating unknown individuals over the Internet, Merchants should look to services or information that is capable of reliably identifying a new customer. For instance, the TRANSACT-SECURE™ service by iShopSecure, Inc. is one system that Merchants can use to identify consumers by checking consumer information against credit bureau records. Similarly, for existing customers that have been provided security tokens (such as PINs and passwords), each Merchant should properly educate these customers about the proper use and protection of such tokens.

D. Record Retention Requirements

All signed or authenticated authorizations must be retained by Merchant for two (2) years after the completion of the transaction or revocation of a recurring transaction authorization. In the case of paper authorizations that have been physically signed by a Purchaser, the original authorization or a micro-film equivalent copy must be retained. For authentications made over the telephone, the Internet, or other on-line network, the Merchant must retain a copy of the authorization and a recorded record of the authentication.

E. Receipt Requirements

The authorization elements listed above must appear together and be provided in electronic or hard copy format to the Purchaser for each ACH debit entry initiated to the Purchaser's account, Recurring Transactions excepted. Merchant should prompt the Purchaser to print the authorization and keep a copy for his or her records. In the case of Recurring Transactions, the Merchant need only provide one copy for the first transaction as described above. The Merchant also should be able to reproduce a hard copy of the authorization if requested.

F. Technical Considerations

Merchants using Weblink or ADC posting methods to submit ACH transactions initially as "Auth-Only" transactions should know that submission of ACH transactions as "Auth-only" simply means that the transaction will not automatically be captured or settled and sent to the bank for processing. Once the Purchaser has properly authorized the transaction as discussed above, the Merchant can access the transaction (which will remain in the current batch until voided or captured) and select the capture option, thus enabling the transaction to settle and beginning the required Authorize.Net waiting period for the availability of funds. Merchants should submit eCheck.Net Transactions through the Virtual Terminal only after receipt of authorization from the Purchaser.

VII. Prohibited Activities

The activities and uses related to the use of the eCheck.Net Services listed in this section are strictly prohibited ("**Prohibited Activities**"). This list of Prohibited Activities is not exhaustive and Authorize.Net reserves the right to modify it at any time as described above. Authorize.Net may suspend or terminate the eCheck.Net Service as a result of any Prohibited Activity by Merchant.

A. Prohibited Transactions.

Merchant shall not at any time conduct its business in any manner that directly or indirectly offers, sells, leases, licenses, displays, delivers, advertises, recommends, or promotes any product(s), service(s), data, information, image(s), text and/or other web site content, which is:

(1) unlawful or violates any applicable local, state, national or international law, ordinance or regulation having the force of law (e.g., NACHA regulations) or which may cause Authorize.Net to be subject to investigation, prosecution, or legal action;

(2) defamatory, libelous, slanderous, abusive, threatening or harassing towards others;

(3) a sweepstakes, lottery, raffle, multi-level marketing program, chain letter or pyramid scheme;

(4) an unfair, unlawful or deceptive business practice;

(5) racially or otherwise offensive, hateful, bigoted or intolerant;

(6) in violation of any privacy or data protection law or right;

(7) infringe or violate any patent, copyright, trademark, trade secret, right of publicity or privacy or other proprietary right under the laws of any jurisdiction;

(8) transmit or deliver any material that contains viruses, worms, Trojan horses, time bombs or any other harmful or damaging code, software program or other technology or the means for developing any of the above;

(9) advocate, promote and/or provide assistance in carrying out violence or any other unlawful activity against any persons or any governments, businesses or other entities;

(10) the subject of any government investigation or proceedings;

(11) any form(s) of gambling; or

(12) not consistent with prevailing Internet "Netiquette" standards, as determined by Authorize.Net in its sole discretion.

B. Prohibited Goods or Services.

Merchant shall not use the eCheck.Net Service to provide or promote any of the following goods or services: audio text; business opportunity sales; card registration organizations; check cashing establishments; collection agencies; computer sales, credit restoration or repair agencies; debt consolidation; drug paraphernalia; employment agencies; third party hotel reservation services; illegal products; import/export; investment opportunities; magazine subscriptions; mortgage broker or mortgage reduction services; outbound telemarketing; precious metal/stamp collections; pre-paid phone cards; pornography or adult-oriented material; pyramid sales programs; telephone consultation services; timeshare organizations; or travel certificates or sales or any other business type or industry that Authorize.Net, at its sole discretion, determines to possess excessive risk and provides Merchant with written notice of same. Furthermore, Merchant shall not use the eCheck.Net Service as a bill paying service.

C. No E-mail or Internet (Net)Abuses.

Merchant will not engage in any form of net abuse, including but not limited to: (1) sending any kind of unsolicited or unwelcome email to a substantial number of network users (SPAM mail), anywhere on the Internet; (2) posting a single article or substantially similar articles to an excessive number of newsgroups or mailing lists; (3) repeated or deliberate posting of articles that are off-topic according to the charter of the newsgroup or mail list where such articles are posted; and (4) posting commercial advertising in a conference or newsgroup, unless it is specifically permitted to be posted within that group.

D. Enforcement

Merchant understands that Authorize.Net may investigate any reported occurrence or potential occurrence of a Prohibited Activity and take appropriate action, which depending on the circumstances and severity of any such occurrence may include: (a) issuing a warning to Merchant and taking necessary action to minimize any damage; (b) suspending Merchant's gateway account and right to access and use the eCheck.Net Service; and/or (c) immediately terminating the eCheck.Net Service and Merchant's Agreement with Authorize.Net.

EXHIBIT A

AUTHORIZATION FOR RECURRING DIRECT PAYMENTS (ACH DEBITS)

Joe Merchant

1245 East 5th Street

Anytown, UT 84064

801-555-5555

RE: ACH Authorization for Recurring Charges

In consideration of the goods, products and/or services provided to me by MERCHANT, as listed above, I hereby authorize MERCHANT to initiate a debit entry to my account indicated below at the depository financial institution named below, hereinafter called DEPOSITORY, and to debit the same to such account for the amount and frequency listed below. I acknowledge that the origination of ACH transactions to my account must comply with the provisions of U.S. law.

Depository Bank Name: _____

Branch (City, State, Zip): _____

Account Type and Number

☐ Checking ☐ Savings: _____

Routing Number: _____

Amount: $_____

Frequency: ☐ monthly, ☐ weekly, or ☐ annual basis

Effective Date: ____/____/____ (mm/dd/yyyy)

The specific debit to my account authorized herein may only post on or after the EFFECTIVE DATE listed above, and in no event may the debit transaction post to my account prior to said date. This authorization is to remain in full force and effect until MERCHANT has received written notification from me of termination in such time and in such manner as to afford MERCHANT and DEPOSITORY a reasonable opportunity to act. I may only revoke this authorization by contacting MERCHANT directly at the address and phone number listed above.

Name: _____ Date: _____
(Please Print)

Signature: _____

EXHIBIT B

AUTHORIZATION FOR SINGLE DIRECT PAYMENT (ACH DEBITS)

Joe Merchant

1245 East 5th Street

Anytown, UT 84064

801-555-5555

RE: ACH Authorization

In consideration of the goods, products and/or services provided to me by MERCHANT, as listed above, I hereby authorize MERCHANT to initiate a debit entry to my checking account indicated below at the depository financial institution named below, hereinafter called DEPOSITORY, and to debit the same to such account for the amount listed below. I acknowledge that the origination of ACH transactions to my account must comply with the provisions of U.S. law.

Depository Bank Name: Branch (City, State, Zip):

_____ _____

Account Type and Number Routing Number:

□ Checking □ Savings: _____ _____

Amount: $_____ Effective Date: ____/____/____ (mm/dd/yyyy)

This authorization is to remain in full force and effect for this transaction only, or until such time that my indebtedness to MERCHANT for the amount listed below is fully satisfied. The specific debit to my account authorized herein may only post on or after the EFFECTIVE DATE listed above, and in no event may the debit transaction post to my account prior to said date.

I may only revoke this authorization by contacting MERCHANT directly at the address and phone number listed above, and only in the case that I return the good, product and/or service provided to me by MERCHANT pursuant to their particular return policy in effect the date this authorization is granted.

Name: _____ Date: _____
(Please Print)

Signature: _____

EXHIBIT C

SECURITY AUDIT CHECKLIST

(1) *Physical security to protect against theft, tampering or damage*.

- Critical network, server, and telecommunications equipment should be placed in physically secure locations that permit access only to authorized personnel.
- Firewalls must be fully deployed with secure processes for administering those firewalls.
- Firewalls must protect websites from inappropriate and unauthorized access.
- Disaster recovery plans must be developed and reviewed periodically.

(2) *Personnel and access controls to protect against unauthorized access and use.*

- A formal set of security policies and procedures must be developed that clearly outline the corporate rules governing access to sensitive financial data.
- Hiring procedures should be developed that will, at a minimum, verify application information and check references on new employees that will have access to Purchaser financial information.
- Relevant employees must be educated on information security and company practices and their individual responsibilities.
- Access controls should be in place to:
    - Limit employee access to secure areas and to documents/files that contain Purchaser financial information.
    - Ensure that terminated employees have no access to secure information and areas.
    - Permit visitors to these areas and information only when absolutely necessary and ensure they are accompanied by an employee at all times.
    - Restrict access from external networks to authenticated users (i.e. by passwords or login codes).
    - Ensure that one person acting alone cannot circumvent safeguards, i.e., dual control procedures are in place.
- Procedures and audit trails need to be established to scrutinize activities of users with access to Purchaser information in order to detect anomalies.

(3) *Network security to ensure secure capture, storage and distribution.*

- All Purchaser financial information should be kept behind firewalls and in an area inaccessible from the Internet.
- A data retention schedule should be developed that covers the policies on how to handle the data from the time of capture to destruction.
- Retention schedules should be monitored to ensure that they are being met.
- Purchaser information should only be stored permanently if it is required by law, regulation, rule, or a governing organization.
- Data should not be stored longer than necessary.
- Distribution of Purchaser data should be limited, with procedures and controls in place governing how it is distributed.
- The need for distributing Purchaser data should be reviewed, and all distribution is verified and approved.
- Purchaser data sent across networks must be encrypted.
- Use and regularly update anti-virus software.
- Regularly test security systems and processes.