

A decorative graphic consisting of a dark blue wave shape with a lighter grey shadow underneath, spanning across the top of the page.

Helping Your Financial Institution Meet Compliance Requirements for NACHA IAT

White Paper
May 2010

Table of Contents

INTRODUCTION	3
I INTERNATIONAL ACH TRANSACTIONS	4
1.1 Executive Summary	4
2 INTERNATIONAL ACH TRANSACTIONS WITH EASTNETS	7
2.1 EastNets Approach	7
2.2 Inbound IAT Traffic	7
2.3 Outbound IAT Traffic	8
3 EN.SAFEWATCH.FILTERING FUNCTIONALITY	9
3.1 Functional view en.SafeWatch Filtering	9
3.2 Integrated Alert Management and Workflow	9
3.3 EastNets added value proposition	10

Introduction

This document describes the details around the latest U.S. requirements for International ACH Transactions (IAT). As of September 2009 all financial institutions (FIs) in the must comply with this requirement.

Implementing the IAT standard entry class code is required to comply with the Treasury Department's Office of Foreign Assets Control (OFAC) rules to fight terrorist financing and money laundering. The code also requires companies to change their business processes to comply with the Travel Rules regarding documenting transactions and verifying compliance.



I International ACH Transactions

I.1 Overview

The primary purposes of the International ACH Transactions rules are to:

1. Respond to the request from the Office of Foreign Assets Control (OFAC) to align the NACHA Operating Rules (Rules) with OFAC compliance obligations; and
2. Make it easier for Depository Financial Institutions (RDFIs) to comply with those obligations. This rule:

- Requires Gateway Operators to classify payments that are transmitted to or received from a financial agency outside the territorial jurisdiction of the U.S. as International ACH Transactions (IATs); and
- Includes the Bank Secrecy Act's (BSA) "Travel Rule" information within the international payment format.

Classification of International ACH Transactions

Currently, cross-border applications are used only for ACH transactions that are transmitted internationally through a declared Gateway Operator. Many payments initiated internationally are currently introduced into the U.S. ACH Network through domestic correspondent banking relationships. As a result, international payments are being transmitted as domestic transactions, making it difficult for Depository Financial Institutions (RDFIs) to identify these transactions for purposes of complying with U.S. law.

The new rule will provide a classification of the International ACH Transactions by focusing on where the financial agency that handles the payment transaction

(movement of the funds) is located and not where any other party to the transaction (e.g., the Originator or Receiver) is located. Therefore, certain transactions that are currently sent as PPDs or CCDs, but are actually international transactions, will be sent as IATs.

Structuring the Formats to Comply with U.S. Law

The information currently included within the cross-border payment formats, CBR and PBR, is not sufficient to allow an RDFI to readily identify all parties to an International ACH Transaction in order to comply with OFAC-administered U.S. sanctions policies.

The new IAT format will help RDFIs comply with their obligations under U.S. law by:

- Carrying the additional data requirements included in the BSA's "Travel Rule" (31 C.F.R. 103.33(g)) as requested by OFAC; and
- Containing OFAC Screening Indicators to aid financial institutions in effective interdiction of unlawful transactions.

The rule will allow for identification of International ACH Transactions (inbound and outbound) and provide financial institutions with sufficient information to conduct an efficient review of the transactions as required by U.S. law.

Rules Framework and Implementation

I. Definition of an International ACH Transaction

The change will define an International ACH Transaction as an ACH entry that is part of a payment transaction involving a financial agency's office that is not located in the territorial jurisdiction of the U.S.

Specifically, an office of a financial agency (Financial agency means an entity that is authorized by applicable law to accept deposits or is in the business of issuing money orders or transferring funds) is involved in the payment transaction if it:

- a. Holds an account that is credited or debited as part of a payment transaction; or
- b. Receives funds directly from a Person or makes payment directly to a Person as part of a payment transaction; or
- c. Serves as an intermediary in the settlement of any part of a payment transaction.

The definition of International ACH Transaction focuses on where the financial institution that handles the payment transaction (movement of the funds) is located and not where any other party to the transaction (e.g., the Originator or Receiver) is located.



2. Gateway Operator Definition and Obligations

A Gateway Operator is an ACH Operator or ODFI that acts as an entry or exit point to or from the U.S. ACH Operators and ODFIs in the role of Gateway Operators have specific warranties and obligations related to IAT entries. ACH Operators as Gateway Operators will limit inbound IAT entries to credits and reversals, while ODFIs as Gateway Operators may transmit both credit and debit entries inbound. All Gateway Operators may send credits and debits outbound.

3. Information Transmitted in IAT Formats

- IATs will include the BSA's "Travel Rule" data within the ACH record for compliance with U.S. law.
- IATs will include:
 - A unique Company/Batch Header and Entry Detail Record;
 - Seven required addenda;
 - Two optional addenda for remittance data;
 - A maximum of five addenda for required correspondent bank identification; and
 - The seven required addenda for all returns (plus the one additional addenda record within which specific information related to the return would be included).
- The field requirements in an IAT will be consistent with SWIFT standards for mapping efficiency.
- IAT transactions will include two optional OFAC screening indicators to convey screening results of a potential blocked party by a Gateway Operator and a Correspondent Bank.
 - The Federal Reserve has announced its intention to screen incoming IAT transactions for OFAC compliance.
 - The Electronic Payments Network (EPN), the private-sector ACH Operator, has also announced that it will make available an OFAC screening function to its customer financial institutions as a value-added service.

Financial Institutions Need to Prepare

Every financial institution needs to understand how it is impacted by the new NACHA rule. Given the significance of this rule change, it is essential that financial institutions start now to understand and implement the rule. All areas of your institution should be ready on September 18, 2009 including, but not limited to, operations, compliance, audit, customer service, and vendor management. Education, training, and technical assistance are available from a number of sources, which are listed below. A checklist of recommended operational and compliance action items is also available.

Penalties for non-compliance with OFAC's regulations can be severe. Financial institutions can contract with other parties for ACH processing services, but cannot contract away their liabilities related to OFAC compliance. NACHA and the ACH Operators encourage financial institutions to begin preparations today.

Other Considerations – ACH Benefits

Implementation of the new IAT Standard Entry Class code provides additional benefits. The majority of ACH systems around the world do not distinguish between payments transmitted to consumer and business accounts. The IAT SEC Code will enhance Network processing efficiencies and enable accurate mapping of data between domestic and international payment systems.

The amendment will also make the U.S. ACH Network formats more consistent with other network formats. For example, wire transfer formats currently carry the 'Travel Rule' information to comply with the BSA. The change is also consistent with the field lengths in SWIFT messages to ensure efficient mapping of data.



2 International ACH Transactions with EastNets

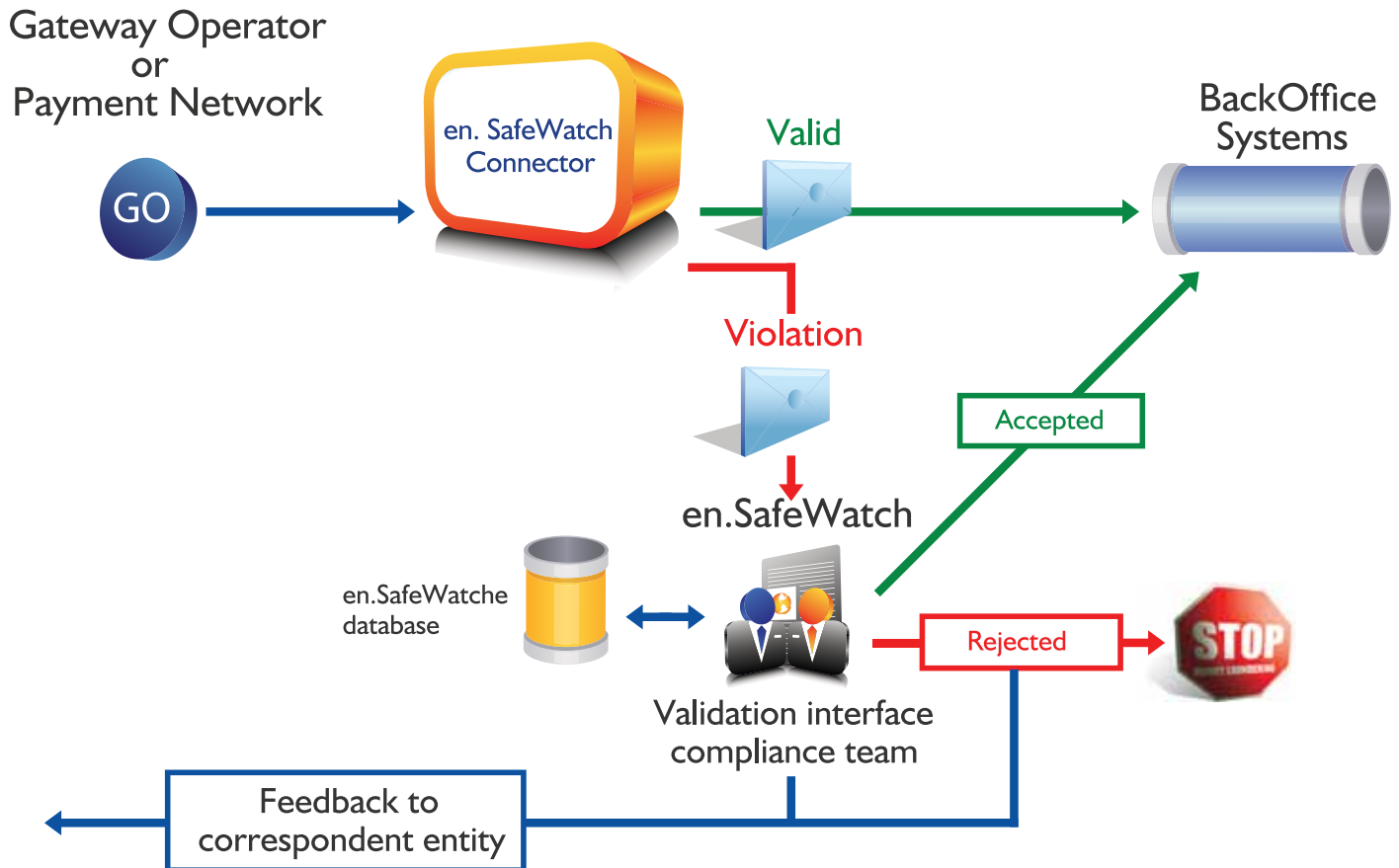
EastNets can help you comply with the NACHA regulations by providing rapidly deployable solutions to detect and check both inbound and outboard IAT traffic. The moment when international traffic is detected, the solution will perform OFAC scanning to cover the specific requirements.

2.1 Scanning Inbound IAT Traffic

U.S. RDFIs and beneficiaries will continue to have an obligation to ensure that all aspects of inbound, cross-border transactions are in compliance with OFAC regulations and to take appropriate steps to investigate, suspend, reject, block and report on transactions as necessary.

EastNets'en.SafeWatch Filtering solution scans all inbound IAT traffic and filters the IATs the moment they come into the RDFIs.

Scanning Inbound RDFI IAT Traffic with EastNets

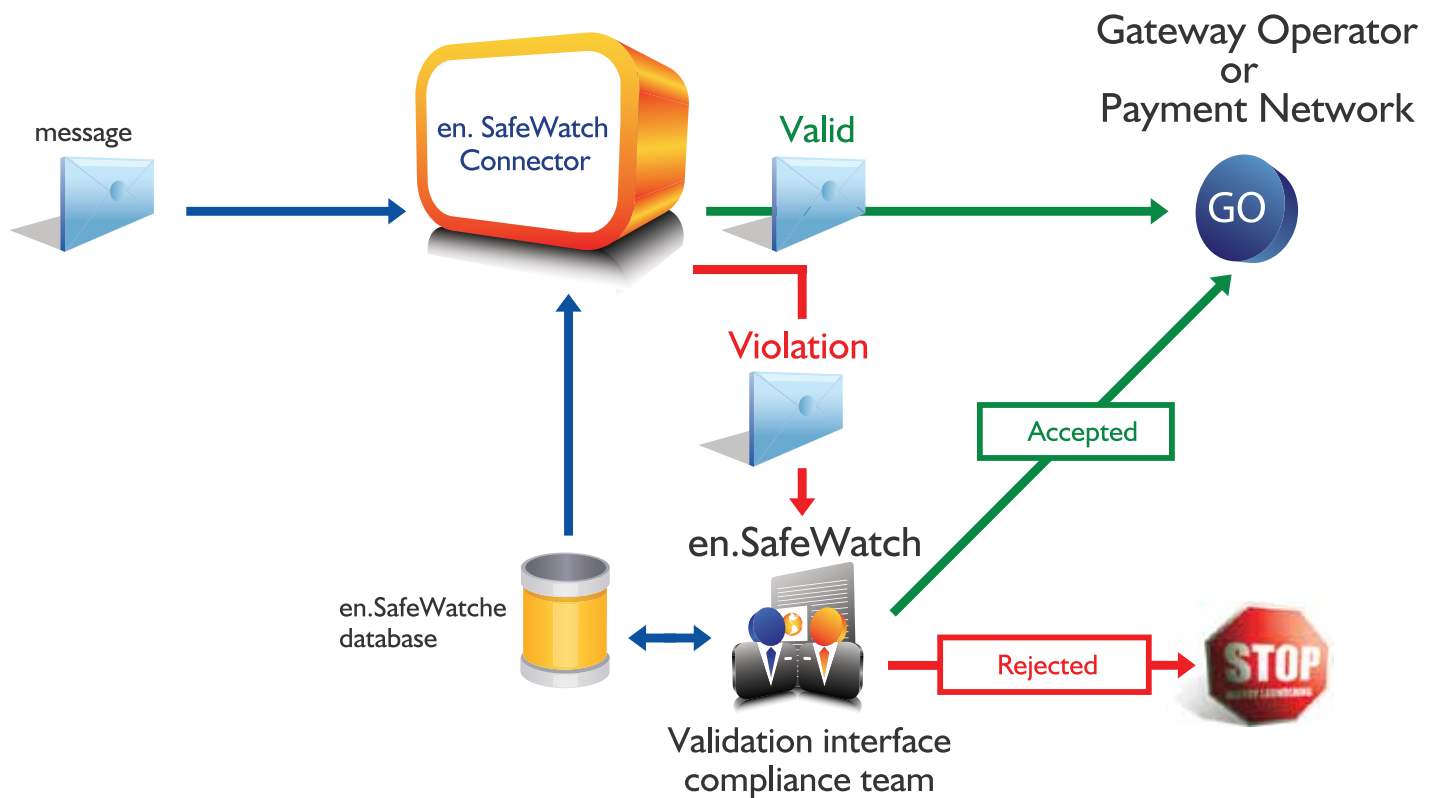


2.2 Scanning Outbound IAT Traffic

U.S. ODFIs and their Originators will continue to be responsible for ensuring that all parties to the transactions, as well as the underlying purpose of the transactions, are not in violation of OFAC regulations. They will need to take appropriate steps to investigate, suspend, reject, block, and report on transactions (Outbound IATs)

EastNets'en.SafeWatch Filtering solution scans all Outbound IAT traffic and filters the IATs just before they are sent to the Automated Clearing House network or payment networks. This avoids problems resulting from technical or functional data errors on a messages or IATs.

Scanning Outbound ODFI IAT Traffic with EastNets

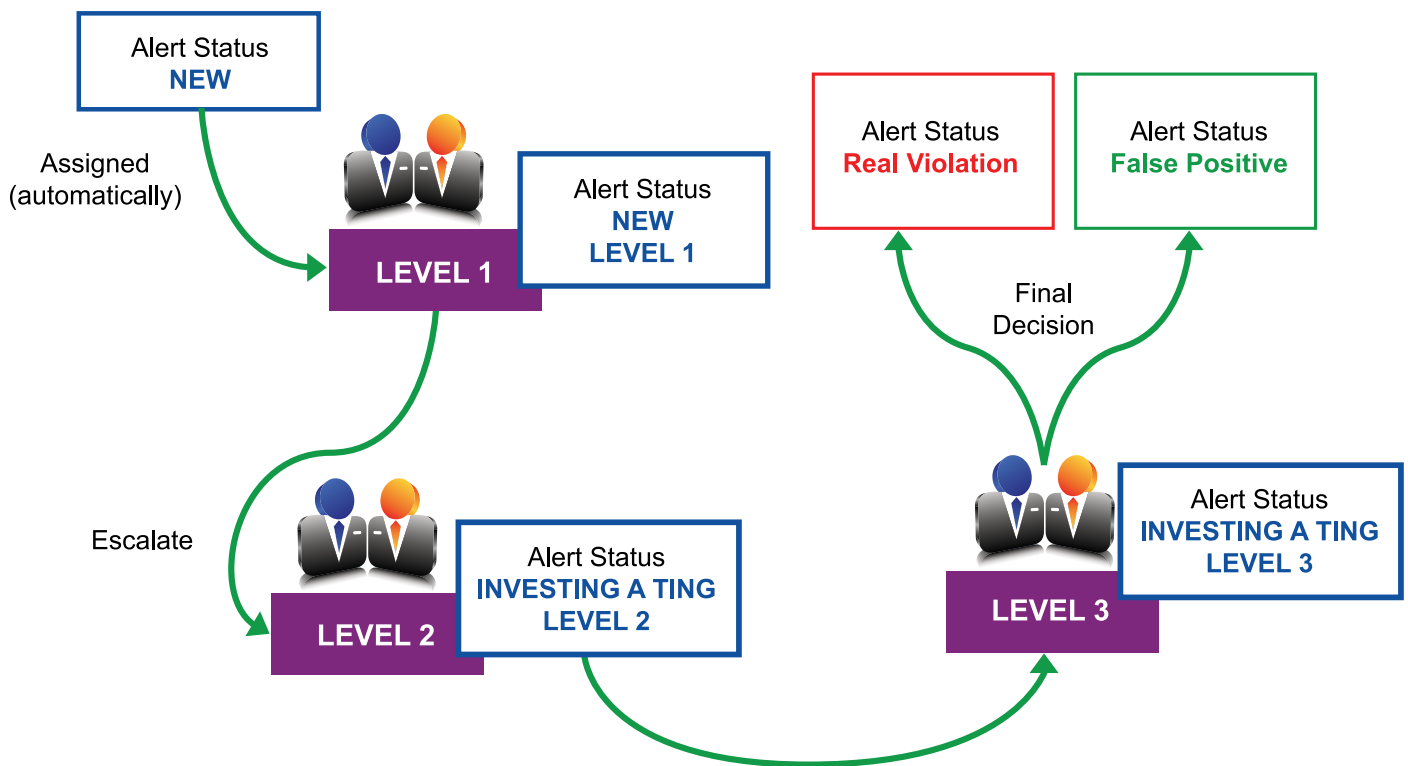


2.3 Integrated Alert Management and Workflow

en.SafeWatch’s integrated alert management and workflow capabilities allow your operator and compliance team to keep track of the activities that they need to perform.

An escalation structure can be configured to meet your team’s needs in order to efficiently and effectively manage incoming detections and alerts.

Multiple Authorization and Escalation Workflows Can be Easily Configured to Meet Your Firm’s Specific Requirements



EastNets added value proposition

EastNets has over 25 years of experience in payment processing and is the market leader for global List Filtering solutions with its en.SafeWatch Filtering solution used today by over 250 customers in 80 countries. Beyond providing the capabilities to help you meet the IAT requirements, EastNets provides value-added capabilities to improve your risk protection and preserve your bottom line.

Improving Risk Protection

- In addition to the OFAC screening of IAT traffic, en.SafeWatch Filtering can provide transaction and/or customer screening for PEP or any other list of your choice.
- Compliance and payments experts can assist you in bringing the best value possible to your system, reducing

your exposure to risk while maintaining fast and reliable ACH/STP processes within your financial institute.

- The en.SafeWatch Filtering solution is also integrated with en.SafeWatch Profiling, a very simple to use, fast to implement and complete offering for transactional and behavioral monitoring of accounts and customers.

Services and Solutions You Can Trust

With our in-depth knowledge and years of experience with financial institutions and regulatory compliance we deliver proven solutions you can trust. EastNets is committed to ensuring you meet your regulatory requirements, and providing ongoing protection for your financial institution.

Copyrights

Copyright© EastNets 2010. All rights reserved.

No parts of this document may be copied or reproduced, even temporarily, in whole or in part, in any manner or form, or on any media, nor sold, licensed, distributed or transferred to any person, or used, adapted, translated, without the prior written permission of EastNets.

The recipient is, however, authorized to copy or reproduce this publication within its own organization if necessary for the purpose for which it is supplied. Any such copy or reproduction will include the following: acknowledgement of the source, reference and date of publication, and all notices set out on this page.

Disclaimer

Although EastNets has made every effort to make this document accurate, up-to-date, and complete, EastNets offers no warranties, express or implied, related to this document. In no event shall EastNets be liable for any loss of profits, loss of business, loss of use or data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind arising from any error in this document.

Send us your comments

EastNets welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important to us.

If you find any errors or have any other suggestions to improve the document quality and clarity, please indicate the chapter and page number (if available).

Please send comments to: info@eastnets.com



450 Seventh Avenue, Suite 1509
NEW YORK, NY 10123
UNITED STATES
Tel: +1 212 631 0666
Fax: +1 212 631 0170
www.eastnets.com

About EastNets

EastNets is a leading provider of global compliance and payment solutions and services with over 900 customers in 120 countries. Founded in 1984, EastNets has over 25 years of experience serving financial institutions, corporates and government agencies around the globe. EastNets provides anti-money laundering, payment and Kiosk solutions, and SWIFT plug-ins and services for SWIFT Connectivity. Through its outsourced fully-hosted Service Bureau, EastNets provides SWIFT connectivity and add-on services for over 200 financial institutions. For more information, please visit www.eastnets.com.