

white paper

RISK
MANAGEMENT

PRESENTED BY THE
RISK & FRAUD
MANAGEMENT COMMITTEE
OF THE ELECTRONIC
TRANSACTIONS
ASSOCIATION

Volume 1 Issue 1
March 10, 2005





Risk Management

ELECTRONIC TRANSACTIONS
ASSOCIATION 2004-2005 RISK & FRAUD
MANAGEMENT COMMITTEE

Ms. Mary F. Dees, Chair
President & CEO
creditranz.com
5068 W Plano Parkway, Suite 300
Plano, TX 75093
(972) 392-7594
fax: (972) 692-7328
mdees@creditranz.com

Jeffry A. Beene (Jeff)
Executive Vice President
Operations & Compliance
Pipeline Data Processing, Inc.
4400 North Point Parkway , Suite 190
Alpharetta, GA 30022
(678) 325-2602 ext. 101
fax: (678) 325-2606
jeff.beene@pipelinedata.com

Barrie Berman VanBrackle
Partner
Mannatt, Phelps & Phillips, LLC
1501 M Street, NW
Washington, DC 20005
(202) 463-4330
fax: (202) 463-1704
bberman@manatt.com

Mike Love
Managing Director
ReD Consulting
508 Main Street
PO Box 669
Marble Falls, TX 75654
(830) 693-6646
fax: (830) 693-6894
mlove@ReDconsulting.com

Tad Scales, Senior Manager
Deloitte & Touche
1111 Broadway, 21st Floor
Oakland, CA
(510) 287-2776
fax: (415) 783-8244
tscales@deloitte.com

William Higgins (Bill)
President & CEO
Retriever Payment Solutions
20405 State Highway 249, Suite 700
Houston, TX 77070
(281) 376-3399
fax: (281) 320-5000
bhiggins@rpsionline.com

Laurie LeBoeuf Novacek
Senior Vice President
Merchant Choice Card Services
16211 Park Ten Place
Houston, TX 77084
(281)579-4438
fax: (281)579-4499
lnovacek@deltacard.com

Eduardo Perez
VISA U.S.A., Inc.
P.O. Box 8999
San Francisco, CA 94128-8999
(650) 432-2375
fax: (650) 432-8510
edperez@visa.com

Steven Peisner
Vice President
Merchant Mechanix
23875 W. Ventura Boulavard , Suite 202-A
Calabasas, CA 91302
(818) 591-9099
fax: (818) 878-9979
steven@aqsl.com" steven@aqsl.com

Staff Liaison
Carla Balakgie
Executive Director
Electronic Transactions Association
1101 16th Street, NW, Suite 402
Washington, DC 20036
(202) 828-2635 ext. 102
fax: (202) 828-2639
carla.balakgie@electron.org

This is the first in a series of white papers authored by the ETA Risk & Fraud Management Committee designed to inform ETA members about industry trends in managing risk within their respective portfolios. The desired outcome is to improve risk management practices among all of our members and to potentially reduce losses within the industry.

Changing technology and markets (such as internet providers, wireless card readers etc) are evolving at a rate that challenges even the best risk management process. These white papers are designed to provide most current information available about best practices as well as loss trends in the marketplace.

We recognize that each acquirer and financial institution has different levels of risk they are willing to accept into their portfolios. This series is not designed to inhibit or restrict the type of risk one should accept, but rather to provide tools that will enable you to better assess and monitor risk within the constraints established by your organization. The practices contained in the upcoming series of articles, are generally considered "best practices" and will be provided by a team of industry experts from a variety of backgrounds in the card industry.

Defining Risk Management

To begin, Risk Management is typically defined in the four major categories listed in bold letters below:

	Business Risk	Fraud Risk
Credit Screening	prevention	prevention
Risk Monitoring	detection	detection

A good system of risk management consists of controls that enable prevention (or reduction) of risk yet facilitates the acquisition of business into your portfolio that fits your risk constraints. A good credit screening system will also identify those businesses that have potential for resulting in losses regardless of cause (either business risk or committing fraud). Alternatively, good detective controls enable early identification of trends that can minimize loss potential if the credit screen process did not identify the potential for either business or fraud risk.

For example, a rigorous credit analysis complete with a "credit report" from a known reporting agency may assist in early identification of a business or owner that has resulted in a loss to an acquirer or financial institution. Although certain card companies require reporting known offenders to a shared database, not every fraud offense is reported. This sometimes results in a single merchant going from acquirer to acquirer, leaving behind a wake of fraud losses. Once a merchant is approved, a failure of the monitoring systems to detect anomalies such as significant increases of chargebacks or unusual increases in sales volume may result in more losses. With the resulting increase in the rate of Internet commerce, it brings with it new risk since the card may be charged prior to fulfilling the cardholder's order. If the issue is not detected early, there is a potential for loss exposure if the merchant ultimately has business failure or if it is determined they have committed fraud.

Certainly a minimum baseline for "best practices" in credit screening can start with what is currently required by the card associations and by law.

Credit Screening Requirements

- ▶ An acquirer must determine that a prospective merchant is financially responsible and there is no significant derogatory background information about any of its principles. This may be done through the below tools:
 - Credit reports
 - Personal and business financial statements
 - Income tax returns
 - Other information lawfully available to the acquirer

- ▶ An Inquiry must be made to the MasterCard Member Alert to Control Merchants (MATCH) system to determine if the prospective merchant has been terminated for cause.

- ▶ Whenever feasible, conduct a physical inspection of the business premises and records to ensure the merchant has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit to conduct business. For mail/phone order merchants, the acquirer must obtain a detailed business description.

- ▶ In addition to the above if the merchant is an electronic commerce merchant the acquirer must examine the merchant's web site to:
 - Verify that the merchant is operating within the acquirers jurisdiction
 - Ensure that the merchant is not engaged in any activity that is in violation of the associations guidelines

- ▶ Ensure that the merchant is not engaged in any illegal activity
Annually:
 - Examine the merchant website
 - Print and retain copies of the website
 - Provide retained copies of the website if so required by the associations

Both associations may audit an acquirer for compliance with the merchant screening requirements. If it is determined that a member has violated the procedures they may assess that member for each merchant agreement not in compliance. In addition the violators are subject to chargebacks of fraudulent transactions.

Subsequent white papers will address other areas of risk management and fraud monitoring hopefully providing value and minimizing overall losses for ETA members.



Electronic Transactions
Association
1101 16th Street NW
Suite 402
Washington, DC 20036
1101 16th Street, NW

(202) 828-2635
Fax 202-828-2639