

BITS

FINANCIAL SERVICES
R O U N D T A B L E

**** Table of Contents and Executive Summary extracted
from the full members-only white paper. ****

ONGOING MONITORING AND SCREENING OF ACH ACTIVITY

**A PUBLICATION OF THE
BITS FRAUD STEERING COMMITTEE**

July 2, 2008

FOR BITS MEMBERS ONLY

**BITS
The Financial Services Roundtable
1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, D.C. 20004
(202) 289-4322
WWW.BITSINFO.ORG**

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	3
OVERVIEW	5
FRAUD RISKS TO THE ACH	9
Origination Fraud.....	9
Insider Origination Fraud	32
Reverse Phishing.....	35
Penny Deposit Fraud	38
Trial Deposit Fraud.....	40
Cross-Channel Fraud Schemes Involving The Ach.....	43
Increased Risk Associated With Third-Party Service Providers.....	46
EMERGING ACH PROCESSES, TECHNOLOGIES, AND THREATS	48
Decoupled Debit Cards.....	48
Secure Vault Payments (SVP) Pilot	57
Remote Deposit Capture (RDC) and Back Office Conversion (BOC) Convergence.....	58
SYSTEM LEVEL INITIATIVES.....	59
New Federal Reserve Forum for Retail Payments Risk Management.....	59
Current NACHA Anti-Fraud Initiatives.....	59
Penny Deposit Fraud and Trial Deposit Fraud	61
Check Counterfeit Potential Action: Potential Industry Level Solution	61
Offsetting entry transaction code initiative	62
ACKNOWLEDGEMENTS	63
ABOUT BITS AND THE BITS FRAUD PROGRAM.....	64
APPENDIX ONE: Taking Stock of Your Own ACH Originating and Receiving Environment	65
APPENDIX TWO: NACHA Rules Interpretation-Use of SEC Codes; Aggregation of Transactions	67
APPENDIX THREE: Non-recurring ACH Payment Application Definitions.....	69
APPENDIX FOUR: ACH Participants.....	71
APPENDIX FIVE: Regulation E Procedures When EFT Service Provider Is Not Holding Consumer's Account.....	73
APPENDIX SIX: OCC Bulletin 2006-39.....	75
APPENDIX SEVEN: OCC Bulletin 2008-12.....	90

EXECUTIVE SUMMARY

The sharp increase in non-recurring ACH transactions has changed the way many financial institutions view and manage ACH fraud. As a consequence, financial institutions have devoted significantly more resources to the detection and mitigation of ACH fraud on both the originating and receiving side of the business. That said, compared with other electronic payment instruments, the industry is still on a significant learning curve when it comes to the nuts and bolts of ACH fraud detection and mitigation. The slope of that learning curve has been made steeper because of the increasing sophistication of fraudsters, the emergence of cross-channel fraud, and the significant increase in socially engineered fraud.

One of the biggest surprises in preparing this paper was the realization that there are significant differences from institution to institution around the kinds of ACH fraud each financial institution is currently best able to detect and prevent. This paper should help level the playing field in that regard. By design, it dives into the mechanics of detecting and mitigating ACH-related fraud. Before taking that dive, it may be useful to enumerate several important points that might be gleaned from the work overall:

- It is impossible to overstate the importance of following both the spirit and letter of the OCC's September 1 2006 regulatory guidance on ACH origination. This guidance was updated in April 2008 to provide additional context around third-party processors and high risk activities, such as telemarketing. Many origination frauds result because of inadequate due diligence, in particular by intermediate sales agents used to recruit new business on behalf of financial services firms.
- The increasing occurrence of socially engineered fraud is making it more important than ever to insure that ACH transactions are initiated by true customers. While there is no such thing as perfect authentication, the ACH has historically required less robust forms of retail authentication than other retail electronic payments applications. The challenge for our industry is how to best raise the bar in this area while still preserving the basic ACH economic model.
- There are several examples in this paper of regularly occurring, but low loss level, fraud. Financial institutions may believe that there is no economically viable means to detect and prevent fraud in these areas, but we have been impressed with the ability of financial institutions to find effective, low cost work-arounds. Hopefully, some of the approaches detailed in this paper can become widespread.
- As expected, the group's work confirmed that ACH transactions are increasingly evident in cross-channel payments fraud schemes. Financial Institutions should continue to take steps to integrate their fraud detection capabilities across payments functions to provide improved customer-centric fraud protection.
- At the time this paper was written, our industry was carefully watching decoupled debit rollouts and eyeing the potential for points of compromise. Although one of the two decoupled debit issuing banks has suspended its pilot program, the work completed by this

project team serves as an important guide to potential risks. One potential area of decoupled debit fraud relates to the practical divergence between Regulation E prescribed practice and actual financial institution procedures when a deposit account customer reports a decoupled debit issue on a card issued elsewhere. This area deserves continuing attention because it is applicable to all ACH debit cards not issued directly by the receiving depository financial institution (RDFI), and there are many such programs.

- The paper explores areas where new industry-wide initiatives might effectively reduce fraud that has thus far been difficult to control. Substantially expanding the use of positive pay and rethinking the existing use of pre-notes are two areas where relatively simple solutions might significantly reduce fraud.

Readers will quickly see a rhythm to the paper, with sections devoted to specific types of fraud organized in a recurring pattern. Most sections begin with a high level overview describing the type of fraud under review, followed by details and specific characteristics of that fraud. Specific examples are provided when members felt comfortable supplying an anyonomized incident – often including details about how the incident was detected and resolved. When financial institutions were not comfortable sharing actual examples, hypothetical examples (clearly labeled) are provided. Examples are followed by more general detection guidance, and close with a section devoted to suggested prevention steps.