



## AML Best Practices Summary For Issuers of Network Branded Prepaid Cards

August 2007

- Develop and implement a comprehensive, customized risk-based AML compliance plan including:
  - An independent risk assessment for each network branded prepaid card product issued or sold
  - Due diligence procedures prior to signing any vendors, sellers, and distributors
  - A customer identification program (CIP) that addresses collecting and verifying customer identification data:
    - CIP is appropriate for network branded prepaid cards that are reloadable and personalized—especially for those that access cash.
    - CIP is generally not necessary for non-reloadable, non-personalized network branded prepaid cards used to purchase goods/services (e.g., gift cards), especially low-dollar amount cards.
    - CIP also may be appropriate for personalized network branded prepaid cards—even those that are not reloadable, depending on an assessment of the risks presented by such products such as the amount of value involved, functionality offered, potential cardholders, and card usage.
  - Enhanced customer due diligence for cardholders who reload their network branded prepaid cards frequently, have cash access, and/or use their cards outside the United States
  - Procedures for filing Currency Transaction Reports (CTRs), if applicable.
  - Procedures for aggregating cash purchases or loads of prepaid cards by the same customer in the same day (for purposes of filing CTRs)
  - Initial and ongoing staff training programs
  - Monitoring transactions and related activities (e.g., loading and card purchasing) for suspicious activity—even if not technically required to do so by law or regulation
  - Identifying reportable transactions and accurately filing Suspicious Activity Reports (SARs)—even if not technically required to do so by law or regulation. Also, for prepaid card issuers, notifying the issuer's Board of all SARs filings.
  - Establishing reasonable record-keeping requirements for large-dollar value network branded prepaid card sales, similar to record-keeping required for monetary instruments—even if not technically required to do so by law or regulation
  - Annual or bi-annual independent compliance audits to ensure compliance at all levels of the organization

- Appoint an AML compliance officer who reports regularly to the issuer’s Board about compliance issues
- Ensure that all sellers and distributors are trained to follow procedures
- Design products to make them unattractive to money launderers:
  - Establish limits on amounts loaded and velocity loads
  - Limit cash access or high dollar amounts to products with “known” customers
  - Monitor use and be willing to cancel the network branded prepaid card if activity is suspicious
- Have an OFAC plan in place for purposes of screening known cardholders before issuing a card, if possible, or shortly thereafter. The OFAC plan should include ongoing and regular screenings to cross-check cardholders against updated SDN Lists and other lists of prohibited persons under OFAC regulations
- Monitor sellers and program for unusual changes in volumes/transactions and/or transactions that fall outside of “usual” program parameters
- Comply with FinCEN Section 314 information requests concerning suspected terrorists and/or money launderers
- Share money laundering and terrorist activity information with other financial institutions after completing appropriate notice procedures with FinCEN and verifying that the receiving/disclosing financial institution has done the same

*The information contained in this Summary is for general guidance on matters of interest only. The information in this Summary is provided with the understanding that the licensors, authors, and publishers are not engaged in rendering legal, accounting, tax, or other professional advice or services. This Summary should not be used as a substitute for consultation with professional accounting, tax, legal, or other competent advisers. Before making any decision or taking any action, you should consult a professional advisor. All information in this Summary is provided “AS IS”, without warranty of any kind, including, but not limited to completeness, accuracy, timeliness, or of the results obtained from use of this information. In no event will the Network Branded Prepaid Card Association, its affiliates, or the members, agents, or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information contained in this Summary or for any consequential, special, or similar damages, even if advised of the possibility of such damages. This disclaimer is subject to applicable law and may not apply, or may apply only to a limited extent, in certain jurisdictions.*



**The Network Branded Prepaid Card Association (NBPCA) is a non-profit inter-industry trade association that supports the growth and success of network branded prepaid cards and represents the common interests of the many participants—including network brands, processors, financial institutions, program managers, distributors, and organizations that support these businesses—in this new and rapidly growing payments category. The NBPCA’s Working Groups drive the activities of the Association for its more than 35 members. For additional information, visit [www.NBPCA.com](http://www.NBPCA.com).**