OCC 2008-12

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: **Payment Processors** Description: **Risk Management Guidance**

Date: April 24, 2008

TO: Chief Executive Officers, Chief Risk Officers and Compliance Officers of All National Banks, Federal Branches and Agencies, Technology Service Providers, Department and Division Heads, and All Examining Personnel

Purpose

This bulletin presents guidance to national banks for due diligence, underwriting, and monitoring of entities that process payments for telemarketers and other merchant clients. As detailed in several OCC issuances, certain merchants, such as telemarketers, pose a higher risk than other merchants and require additional due diligence and close monitoring. This bulletin supplements, but does not replace, existing guidance related to Automated Clearing House (ACH) risk management, merchant processing, and remotely-created checks (RCCs).

Background

The OCC has seen a variety of relationships between banks and processors in which the processor uses its bank relationship to process payments for merchant clients. Often the processor uses a bank account as the vehicle to conduct such payment processing. For example, a processor may be a bank customer that deposits into its account RCCs generated on behalf of merchant clients. A processor may also act as a third-party sender of ACH transactions, originating debits for its merchant clients through its customer relationship with the bank. In either case, the bank often has no direct customer relationship with the merchant. Risks are heightened when neither the processor nor the bank performs adequate due diligence on the merchants for which they are originating payments.

When a bank has a relationship with a processor, it is exposed to risks that may not be present in relationships with other commercial customers. The bank encounters strategic, credit, compliance, transaction, and reputation risks in these relationships. Banks have two distinct areas of responsibility to control these risks. The first is due diligence and underwriting, and the second is monitoring these high-risk accounts for high levels of unauthorized returns and for suspicious or unusual patterns of activity. Proper initial due diligence, effective underwriting, and ongoing account monitoring are critical for bank safety and soundness and consumer protection. Banks should implement these controls

to reduce the likelihood of establishing or maintaining an inappropriate relationship with a processor through which unscrupulous merchants can gain access to consumers' bank accounts.

Banks should also consider carefully the legal, reputation, and other risks presented by relationships with processors including risks associated with customer complaints, returned items, and potential unfair or deceptive practices.[1] Banks that do not have the appropriate controls to address the risks in these relationships may be viewed as facilitating a processor's or its merchant client's fraud or other unlawful activity. Banks should be alert for processors that use more than one bank to process payments for merchant clients and should subject such processors to great scrutiny. Processing through multiple banks may be a signal that the processor recognizes a risk that one or more of these processing relationships may be terminated as a result of suspicious, fraudulent, or other unlawful conduct.[2]

Risk Management: Effective Due Diligence, Underwriting, and Monitoring

The OCC has provided guidance to national banks regarding relationships with processors. For example, banks must implement a due diligence and underwriting policy that, among other things, requires an initial background check of the processor and its underlying merchants to support the validity of the processor's and merchants' businesses, their creditworthiness, and business practices.[3] Moreover, the OCC has also provided banks detailed procedures for merchant underwriting and review, as well as for fraud monitoring.[4] Banks should review carefully the validity and creditworthiness of all processors and merchants. Controls should be more rigorous for higher-risk processors and merchants (*e.g.*, telemarketers). Although some processors may process transactions for reputable telemarketing merchants, these merchants in aggregate have displayed a much higher incidence of unauthorized returns or chargebacks, which is often indicative of fraudulent activity.

Due diligence, underwriting and account monitoring are especially important for banks in which processors deposit RCCs and through which processors initiate ACH transactions for their merchant clients. Banks should be alert to processors' merchant clients that obtain personal bank account information inappropriately. The merchant may have misused the customer information to facilitate the creation of an unauthorized RCC or ACH debit file by the processor.[5] To ensure effective risk management, banks that initiate transactions for processors should require the processor to provide information on their merchant clients such as the merchant's name, principal business activity, and geographic location.[6] Banks should verify directly, or through the processor, that the originator of the payment (*i.e.* the merchant) is operating a legitimate business. Such verification could include comparing the identifying information against public record databases and fraud and bad check databases, comparing the identifying information with information from a trusted third party, such as a credit report from a consumer reporting agency, or checking references from other financial institutions. With respect to account monitoring, a bank should not accept high levels of returns[7] on the basis that the processor has provided collateral or other security to the bank.

By implementing the appropriate controls over processors and their merchant clients, a bank should be able to identify those processors that process for fraudulent telemarketers

or other unscrupulous merchants and to ensure that the bank is not facilitating these transactions. In the event a bank identifies fraudulent or other improper activity with a processor or a specific merchant client of the processor, the bank should take immediate steps to address the problem, including filing a Suspicious Activity Report when appropriate, terminating the bank's relationship with the processor, or requiring the processor to cease processing for that specific merchant.

Banks are required to have Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance programs and appropriate policies, procedures, and processes to monitor and identify unusual activity. Additionally, the FFIEC BSA/AML Examination Manual reiterates the OCC's expectation that banks effectively assess and manage their risks with respect to third-party processors. Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions or transactions prohibited by the Office of Foreign Assets Control. The bank's risk management program should include procedures for monitoring processor information such as merchant data, transaction volume, and charge-back history.[8]

Conclusion

The OCC supports national banks' participation in payment systems to serve the needs of legitimate processors and the customers of such processors and to diversify sources of revenue. However, to limit potential risk to banks and consumers, banks should ensure implementation of risk management programs that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, bank programs should verify the legitimacy of the processor's business operations, assess the bank's risk level, and monitor processor relationships for activity indicative of fraud.

Additional Information

For additional information related to managing the risks associated with retail payment activities please refer to:

- OCC Bulletin 2006-39, ACH Activities: Risk Management Guidance.
- The "Merchant Processing" booklet of the *Comptroller's Handbook*.
- OCC Bulletin 2006-13, Amendments to Regulation CC and J.
- OCC Bulletin 2001-47, Third-Party Relationships: Risk Management Principles.
- The "Outsourcing Technology Services" booklet of the *Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook.*
- The "Retail Payment Systems" booklet of the *FFIEC IT Examination Handbook*.
- The *FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*.

Please direct any questions or comments to the Operational Risk Policy Division at (202) 874-5190.

/signed/

Mark L. O'Dell
Deputy Comptroller for Operational Risk

---

[1] *See* 15 USC 45. See also OCC Advisory Letter 2002-3, Guidance on Unfair or Deceptive Acts or Practices.

[2] *See, e.g.,* OCC Bulletin 2006-39, p.10.

[3] *See* the "Merchant Processing" booklet of the *Comptroller's Handbook*, pp. 24-28, 34; The FFIEC's Bank Secrecy Act/Anti-Money Laundering Examination Manual, Third Party Payment Processors; and OCC Bulletin 2006-39, pp. 5, 10-11.

[4] *See* the "Merchant Processing" booklet of the *Comptroller's Handbook*, pp. 24-28.

[5] Though the Merchant Processing booklet of the Comptroller's Handbook addresses directly merchant card acquiring, its principles and most of the procedures outlined in the handbook are also applicable to the processing of other payment instruments, including RCCs and ACH transactions. *See, e.g.,* OCC Bulletin 2006-39, footnote 7 and associated text.

[6] *See* OCC Bulletin 2006-39. A background check on the principal business owners supplements the underwriting of the merchant client. It is not uncommon for unscrupulous owners to use multiple business entities to avoid detection.

[7] Generally, a bank should not accept high levels of returns regardless of the return reason. High levels of RCCs or ACH debits returned for insufficient funds can be an indication of fraud.

[8] FFIEC BSA/AML Examination Manual, p. 210 (Third-Party Payment Processors). *See also* OCC Bulletin 2006-39.