Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-127-2008
November 7, 2008

GUIDANCE ON PAYMENT PROCESSOR RELATIONSHIPS

Summary: The FDIC is issuing the attached guidance that describes potential risks associated with relationships with entities that process payments for telemarketers and other merchant clients. These types of relationships pose a higher risk and require additional due diligence and close monitoring. This guidance outlines risk management principles for this type of higher-risk activity.

Distribution:
FDIC-supervised Institutions

Suggested Routing:
Chief Executive Officer
Executive Officers
BSA Compliance Officer

Related Topics:
Risk Management
FDIC Guidance for Managing Third-Party Risk (FIL 44-2008, June 2008)
FFIEC Handbook on Retail Payment Systems (March 2004)
FFIEC Handbook on Outsourcing Technology Services (June 2004)
FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual

Attachment:
Guidance on Payment Processor Relationships

Contact:
Michael Benardo, Chief, Cyber Fraud and Financial Crimes Section, at mbenardo@fdic.gov or (202) 898-7319

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2008/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- Account relationships with entities that process payments for telemarketers and other merchant clients could expose financial institutions to increased strategic, credit, compliance, transaction, and reputation risks.
- Account relationships with these higher-risk entities require careful due diligence and monitoring as well as prudent and effective underwriting.
- Payment processors pose greater money laundering and fraud risk if they do not have an effective means of verifying their merchant clients' identities and business practices.
- A financial institution should assess its risk tolerance for this type of activity as part of its risk management program and develop policies and procedures that address due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships for suspicious activity.
- Financial institutions should be alert to consumer complaints that suggest a payment processor's merchant clients are inappropriately obtaining personal account information.
- Financial institutions should act promptly when they believe fraudulent or improper activities have occurred related to a payment processor.

GUIDANCE ON PAYMENT PROCESSOR RELATIONSHIPS

The FDIC has seen an increase in the number of relationships between financial institutions and payment processors in which the payment processor is a deposit customer of the financial institution and uses its customer relationship to process payments for merchant clients. Most payment processors effect transactions that are legitimate payments for a variety of reputable merchants. However, telemarketing and online merchants, in the aggregate, have displayed a higher incidence of unauthorized charges and associated returns or charge backs, which is often indicative of fraudulent activity. Payment processors pose greater money laundering and fraud risk if they do not have an effective means of verifying their merchant clients' identities and business practices. In these cases, financial institutions should perform enhanced due diligence and heightened account monitoring.

Payment processors typically process payments by creating and depositing remotely created checks (RCCs)—often referred to as "Demand Drafts"—or by originating Automated Clearing House (ACH) debits on behalf of their merchant customers. The payment processor may use its own deposit account to process such transactions, or it may establish deposit accounts for its merchant clients to process transactions. Although all the core elements of managing third-party risk are present in payment processor relationships (e.g., risk assessment, due diligence, and oversight), managing this risk where there may not be a direct customer relationship with the merchant can present challenges for financial institutions. Risks associated with this type of activity are heightened when neither the payment processor nor the financial institution performs adequate due diligence on the merchants for which payments are originated.

Potential Risks Arising from Payment Processor Relationships

Deposit relationships with payment processors expose financial institutions to risks that may not be present in relationships with other commercial customers, including increased strategic, credit, compliance, and transaction risks. In addition, financial institutions also should consider the potential for legal, reputation, and other risks presented by relationships with payment processors, including those associated with customer complaints, returned items, and potential unfair or deceptive practices. Financial institutions that do not adequately manage these relationships may be viewed as facilitating fraudulent or unlawful activity by a payment processor or merchant client. Therefore, it is imperative that financial institutions recognize and understand the businesses with which they are involved.

Financial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments. Processors may use multiple financial institutions because they recognize that one or more of the relationships may be terminated as a result of suspicious activity.

Financial institutions also should be alert to consumer complaints that suggest a payment processor's merchant clients are inappropriately obtaining personal account information and using it to create unauthorized RCCs or ACH debits.

Financial institutions should act promptly when they believe fraudulent or improper activities have occurred related to activities of a payment processor. Appropriate actions may include, but are not limited to, filing a Suspicious Activity Report, requiring the payment processor to cease processing for that specific merchant, or terminating the financial institution's relationship with the payment processor.

Risk Management Controls

Financial institutions should establish clear lines of responsibility for controlling risks associated with payment processor relationships. These include effective due diligence and underwriting, as well as ongoing monitoring of high-risk accounts for an increase in unauthorized returns and suspicious activity. Implementing appropriate controls over payment processors and their merchant clients will help identify those payment processors that process items for fraudulent telemarketers or other unscrupulous merchants and help ensure that the financial institution does not facilitate these transactions. Due diligence, underwriting, and account monitoring are especially important for financial institutions in which processors deposit RCCs and through which processors initiate ACH transactions for their merchant clients.

Due Diligence and Underwriting

Due diligence and effective underwriting are critical for an effective risk management program. Financial institutions should implement policies and procedures to reduce the likelihood of establishing or maintaining an inappropriate relationship with a payment processor through which unscrupulous merchants can access customers' deposit accounts.

Financial institutions that initiate transactions for payment processors should develop a processor approval program that extends beyond credit risk management. This program should include a due diligence and underwriting policy that, among other things, requires a background check of the payment processor and its merchant clients. This will help validate the activities, creditworthiness, and business practices of the payment processor. At a minimum, the policy should authenticate the processor's business operations and assess the entity's risk level. An assessment of the processor should include:

- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele.[1]

[1] Businesses with elevated risk may include offshore companies, on-line gambling-related operations, and on-line payday lenders. For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.

- Determining if the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization opportunities" or "gateway" arrangements".[2]

- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants.

- Identifying the major lines of business and volume for the processor's customers.

- Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners.

- Visiting the processor's business operations center.

Financial institutions should require the payment processor to provide information on its merchant clients, such as the merchant's name, principal business activity, geographic location, and sales techniques. Financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record and fraud databases and a trusted third party, such as a credit report from a consumer reporting agency or the state Better Business Bureau, or checking references from other financial institutions.

Ongoing Monitoring

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs, which often are evidence of fraudulent activity. High levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds can be an indication of fraud.

Financial institutions are required to have a Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program and appropriate policies, procedures, and processes in place for monitoring, detecting, and reporting suspicious activity. Non-bank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The FFIEC BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk with respect to third-party payment processors and, as a result, a financial institution's risk management program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.

[2] An Independent Sales Organization is an outside company contracted to procure new merchant relationships. Gateway arrangements are similar to Internet service providers that sell excess computer storage capacity to third parties, who in turn distribute computer services to other individuals unknown to the provider. The third party would make decisions about who would be receiving the service, although the provider would be responsible for the ultimate storage capacity.

Evolving Legal Framework for Remotely Created Checks

The laws and regulations governing the acceptance of RCCs are continually evolving in response to new fraud techniques, technological advancements, increased use of image-based processing, and other factors. As such, financial institutions should ensure that payment processors and their merchants are aware of and comply with the legal/regulatory framework governing these payments and have in place a process to remain informed of changes to applicable laws and regulations, such as:

- Changes to Federal Reserve Bank Operating Circular 3 that clarify electronically created images (including RCC items) that were not originally captured from paper are not eligible to be processed as Check 21 items (effective July 15, 2008).[3]

- Changes to Regulation CC that establish transfer and presentment warranties for RCC items that effectively return the responsibility for ensuring a check is authorized by the account holder to the bank of first deposit (effective July 1, 2006).[4]

- Rules and regulations governing the applicable ACH payment transactions.[5]

- Rules governing the use of telemarketing that require verifiable authorization of payment for services.[6]

Conclusion

The FDIC supports financial institutions' participation in payment systems to serve the needs of legitimate payment processors and their merchant clients. However, to limit potential risks, financial institutions should implement risk management policies and procedures that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, risk management programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, and monitor payment processor relationships for suspicious activity. Financial institutions should act promptly if they believe fraudulent or improper activities have occurred related to activities of a payment processor.

[3] Federal Reserve Banks Operating Circular No. 3 - Collection of Cash Items and Returned Checks, www.frbservices.org/files/regulations/pdf/operating_circular_3.pdf.
[4] Effective July 1, 2006 [70 Fed. Reg. 71218-71226 (November 28, 2005)].
[5] NACHA [www.nacha.org/ACH_Rules/ach_rules.htm].
[6] Federal Trade Commission Telemarketing Sales Rule [16 CFR 310].