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

Financial Institution Letter
FIL-3-2012
January 31, 2012

Payment Processor Relationships
Revised Guidance

Summary: Attached is revised guidance describing potential risks associated with relationships with third-party entities that process payments for telemarketers, online businesses, and other merchants (collectively "merchants"). These relationships can pose increased risk to institutions and require careful due diligence and monitoring. This guidance outlines certain risk mitigation principles for this type of activity.

Statement of Applicability to Institutions with Total Assets under $1 Billion: This guidance applies to all FDIC-supervised financial institutions that have relationships with third-party payment processors.

Distribution:
FDIC-Supervised Institutions

Suggested Routing:
Chief Executive Officer
Executive Officers
Compliance Officer
Chief Information Officer
BSA Officer

Related Topics:
Guidance on Payment Processor Relationships (FIL 127-2008, November 2008)
Consumer Protection, Compliance Risk, and Risk Management
FDIC Guidance for Managing Third-Party Risk (FIL 44-2008, June 2008)
FFIEC Handbook on Retail Payment Systems (February 2010)
FFIEC Handbook on Outsourcing Technology Services (June 2004)
FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual (April 2010)
Managing Risks in Third-Party Payment Processor Relationships (Summer 2011 Supervisory Insights Journal)

Attachment:
Revised Guidance on Payment Processor Relationships

Contacts:
Kathryn Weatherby, Examination Specialist (Fraud), Division of Risk Management Supervision, at kweatherby@fdic.gov or (703) 254-0469

John Bowman, Review Examiner, Division of Depositor and Consumer Protection, at jbowman@fdic.gov or (202) 898-6574

Note:
FDIC Financial Institution Letters may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2012/index.html.

To receive Financial Institution Letters electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html. Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (877-275-3342 or 703-562-2200).

Highlights:

- Account relationships with third-party entities that process payments for merchants require careful due diligence, close monitoring, and prudent underwriting.
- Account relationships with high-risk entities pose increased risks, including potentially unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act.
- Certain types of payment processors may pose heightened money laundering and fraud risks if merchant client identities are not verified and business practices are not reviewed.
- Financial institutions should assess risk tolerance in their overall risk assessment program and develop policies and procedures addressing due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships.
- Financial institutions should be alert to consumer complaints or unusual return rates that suggest the inappropriate use of personal account information and possible deception or unfair treatment of consumers.
- Financial institutions should act promptly when fraudulent or improper activities occur relating to a payment processor, including possibly terminating the relationship.
- Improperly managing these risks may result in the imposition of enforcement actions, such as civil money penalties or restitution orders.

Financial Institution Letter
FIL-3-2012
January 31, 2012

Revised Guidance on Payment Processor Relationships

The FDIC has recently seen an increase in the number of relationships between financial institutions and payment processors in which the payment processor, who is a deposit customer of the financial institution, uses its relationship to process payments for third-party merchant clients. Payment processors typically process payments either 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.

While payment processors generally effect legitimate payment transactions for reputable merchants, the risk profile of such entities can vary significantly depending on the make-up of their customer base. For example, payment processors that deal with telemarketing and online merchants[1] may have a higher risk profile because such entities have tended to display a higher incidence of consumer fraud or potentially illegal activities than some other businesses. Given this variability of risk, payment processors must have effective processes for verifying their merchant clients' identities and reviewing their business practices. Payment processors that do not have such processes can pose elevated money laundering and fraud risk for financial institutions, as well as legal, reputational, and compliance risks if consumers are harmed.

Financial institutions should understand, verify, and monitor the activities and the entities related to the account relationship. Although all of the core elements of managing third-party risk should be considered in payment processor relationships (e.g., risk assessment, due diligence, and oversight), managing this risk poses an increased challenge for the financial institution when there may not be a direct customer relationship with the merchant. For example, it may be difficult to obtain necessary information from the payment processor, particularly if a merchant is also a payment processor, resulting in a "nested" payment processor or "aggregator" relationship.

Financial institutions should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. These agreements should also protect financial institutions by providing for immediate account closure, contract termination, or similar action, as well as establishing adequate reserve requirements to cover anticipated charge backs. Accordingly, financial institutions should perform due diligence and account monitoring appropriate to the risk posed by the payment processor and its merchant

[1] Examples of telemarketing, online businesses, and other merchants that may have a higher incidence of consumer fraud or potentially illegal activities or may otherwise pose elevated risk include credit repair services, debt consolidation and forgiveness programs, online gambling-related operations, government grant or will-writing kits, payday or subprime loans, pornography, online tobacco or firearms sales, pharmaceutical sales, sweepstakes, and magazine subscriptions. This list is not all-inclusive.

base. Risks associated with this type of activity are further increased if neither the payment processor nor the financial institution performs adequate due diligence on the merchants for which payments are originated. Financial institutions are reminded that they cannot rely solely on due diligence performed by the payment processor. The FDIC expects a financial institution to adequately oversee all transactions and activities that it processes and to appropriately manage and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks, among others.

Potential Risks Arising from Payment Processor Relationships

Deposit relationships with payment processors expose financial institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks. In addition, financial institutions should consider the potential for legal, reputational, and other risks, including risks associated with a high or increasing number of customer complaints and returned items, and the potential for claims of unfair or deceptive practices. *Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices.* In such cases, the financial institution and responsible individuals have been subject to a variety of enforcement and other actions. Financial institutions must recognize and understand the businesses and customers with which they have relationships and the liability risk for facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act.[2]

Financial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments or that have a history of moving from one financial institution to another within a short period. 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 should also be on alert for payment processors that solicit business relationships with troubled financial institutions in need of capital. In such cases, payment processors will identify and establish relationships with troubled financial institutions because these financial institutions may be more willing to engage in higher-risk transactions in exchange for increased fee income. In some cases, payment processors have also committed to purchasing stock in certain troubled financial institutions or have guaranteed to place a large deposit with the financial institution, thereby providing additional, much-needed capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

[2] Under Section 8 of the Federal Deposit Insurance Act, the FDIC has authority to enforce the prohibitions against Unfair or Deceptive Acts or Practices (UDAP) in the Federal Trade Commission Act. UDAP violations can result in unsatisfactory Community Reinvestment Act ratings, compliance rating downgrades, restitution to consumers, and the pursuit of civil money penalties.

Financial institutions also should be alert to an increase in consumer complaints about payment processors and/or merchant clients or an increase in the amount of returns or charge backs, all of which may suggest that the originating merchant may be engaged in unfair or deceptive practices or may be inappropriately obtaining or using consumers' personal account information to create unauthorized RCCs or ACH debits. Consumer complaints may be made to a variety of sources and not just directly to the financial institution. They may be sent to the payment processor or the underlying merchant, or directed to consumer advocacy groups or online complaint Web sites or blogs. Financial institutions should take reasonable steps to ensure they understand the type and level of complaints related to transactions that it processes. Financial institutions should also determine, to the extent possible, if there are any external investigations of or legal actions against a processor or its owners and operators during initial and ongoing due diligence of payment processors.

Financial institutions should act promptly to minimize possible consumer harm, particularly in cases involving potentially fraudulent or improper activities relating to activities of a payment processor or its merchant clients. Appropriate actions include filing a Suspicious Activity Report,[3] requiring the payment processor to cease processing for a specific merchant, freezing certain deposit account balances to cover anticipated charge backs, and/or terminating the financial institution's relationship with the payment processor.

Risk Mitigation

Financial institutions should delineate clear lines of responsibility for controlling risks associated with payment processor relationships. Controls may include enhanced due diligence; effective underwriting; and increased scrutiny and monitoring of high-risk accounts for an increase in unauthorized returns, charge backs, suspicious activity, and/or consumer complaints. Implementing appropriate controls for payment processors and their merchant clients can help identify payment processors that process items for fraudulent telemarketers, online scammers, or other unscrupulous merchants and help ensure that the financial institution is not facilitating these transactions. Appropriate oversight and monitoring of these accounts may require the involvement of multiple departments, including information technology, operations, BSA/anti-money laundering (AML), and compliance.

Due Diligence and Underwriting

Financial institutions should implement policies and procedures designed to reduce the likelihood of establishing or maintaining inappropriate relationships with payment processors used by unscrupulous merchants. Such policies and procedures should outline the bank's thresholds for unauthorized returns, the possible actions that can be taken against payment processors that exceed these standards, and methods for periodically reporting such activities to the bank's board of directors and senior management.

[3] The U.S. Department of Treasury's Regulation 31 (CFR 103.18) requires that every federally supervised banking organization file a SAR when the institution detects a known or suspected violation of federal law. Part 353 of the FDIC's Rules and Regulations addresses SAR filing requirements and makes them applicable to all state-chartered financial institutions that are not members of the Federal Reserve System.

As part of such policies and procedures, financial institutions 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, its principal owners, and its merchant clients. This will help validate the activities, creditworthiness, and business practices of the payment processor, as well as identify potential problem merchants. Payment processors may also process transactions for other payment processors, resulting in nested payment processors or aggregator relationships. The financial institution should be aware of these activities and obtain data on the nested processor and its merchant clients. Nested processors and aggregator relationships pose additional challenges as they may be extremely difficult to monitor and control; therefore, risk to the institution is significantly elevated in these cases.

Controls and due diligence requirements should be robust for payment processors and their merchant clients. At a minimum, the policies and procedures should authenticate the processor's business operations and assess the entity's risk level. An assessment should include:

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

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

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

- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele;[4]

- Determining if the processor re-sells its services to a third party that may be referred to as an agent or provider of "Independent Sales Organization opportunities" or a "gateway arrangement"[5] and whether due diligence procedures applied to those entities are sufficient;

- Visiting the processor's business operations center;

- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions; and,

- Determining whether any conflicts of interest exist between management and insiders of the financial institution.

[4] See footnote 1 for examples of potentially high-risk areas.

[5] 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.

Financial institutions should require that payment processors provide information on their merchant clients, such as the merchant's name, principal business activity, location, and sales techniques. The same information should be obtained if the merchant uses sub-merchants (often called "affiliates"). Additionally, 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, fraud databases, and a trusted third party, such as a consumer reporting agency or consumer advocacy group, and/or checking references from other financial institutions. The financial institution should also obtain independent operational audits of the payment processor to assess the accuracy and reliability of the processor's systems. The more the financial institution relies on the payment processor for due diligence and monitoring of its merchant client without direct financial institution involvement and verification, the more important it is to have an independent review to ensure that the processor's controls are sufficient and that contractual agreements between the financial institution and the third-party payment processor are honored.

Ongoing Monitoring

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs and/or high levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds, all of which often indicate fraudulent activity. This would include analyzing and monitoring the adequacy of any reserve balances or accounts established to continually cover charge-back activity.

Financial institutions are required to have a BSA/AML compliance program and appropriate policies, procedures, and processes for monitoring, detecting, and reporting suspicious activity. However, nonbank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors are more 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 associated with third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.

Consumer complaints and/or high rates of return may be an indicator of unauthorized or illegal activity. As such, financial institutions should establish procedures for regularly surveying the sources of consumer complaints that may be lodged with the payment processor, its merchant clients or their affiliates, or on publicly available complaint Web sites and/or blogs. This will help the institutions identify processors and merchants that may pose greater risk.

Similarly, financial institutions should have a formalized process for periodically auditing their third-party payment processing relationships; including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.

Conclusion

The FDIC recognizes that financial institutions provide legitimate services for payment processors and their merchant clients. However, to limit potential risks, financial institutions should implement risk mitigation policies and procedures that include oversight and controls appropriate for the risk and transaction types of the payment processing activities. At a minimum, Board-approved policies and programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, determine the character of the payment processor's ownership, and ensure ongoing monitoring of payment processor relationships for suspicious activity, among other things. Adequate routines and controls will include sufficient staffing with the appropriate background and experience for managing third-party payment processing relationships of the size and scope present at the institution, as well as strong oversight and monitoring by the board and senior management. Financial institutions should act promptly if they believe fraudulent or improper activities potentially resulting in consumer harm have occurred related to activities of a payment processor or its merchant clients, in accordance with their duties under BSA/AML policies and procedures, as well as under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts and practices.

Sandra L. Thompson
Director
Division of Risk Management Supervision

Mark Pearce
Director
Division of Depositor and Consumer Protection