Managing Risks in Third-Party Payment Processor Relationships

During the past few years, the Federal Deposit Insurance Corporation (FDIC) has observed an increase in the number of deposit relationships between financial institutions and third-party payment processors and a corresponding increase in the risks associated with these relationships. Deposit relationships with payment processors can expose financial institutions to risks not present in typical commercial customer relationships, including greater strategic, credit, compliance, transaction, legal, and reputation risk. It was for this reason in 2008 that the FDIC issued *Guidance on Payment Processor Relationships* which outlines risk mitigation principles for this type of higher-risk activity.[1]

Although many payment processors effect legitimate payment transactions for a variety of reputable merchants, an increasing number of processors have been initiating payments for abusive telemarketers, deceptive online merchants, and organizations that engage in high risk or illegal activities. In the absence of adequate monitoring systems and controls, a financial institution could be facilitating unauthorized transactions or unfair or deceptive practices resulting in financial harm to the consumer. Therefore, it is essential that financial institutions and examiners recognize and understand the risks associated with these relationships.

This article explains the role of third-party payment processors and the risks they can present to financial institutions, identifies warning signs that may indicate heightened risk in a payment processor relationship, and discusses the risk mitigation controls that should be in place to manage this risk. The article concludes with an overview of supervisory remedies that may be used when it is determined that a financial institution does not have an adequate program in place for monitoring and addressing the risks associated with third-party payment processor relationships.

Background

The core elements of managing third-party risk are present in payment processor relationships (e.g., risk assessment, policies and procedures, due diligence, and oversight). Managing these risks can be particularly challenging as the financial institution does not have a direct customer relationship with the payment processor's merchant clients. Furthermore, the risks associated with this type of activity are heightened when neither the payment processor nor the financial institution performs adequate due diligence, such as verifying the identities and business practices of the merchants for which payments are originated and implementing a program of ongoing monitoring for suspicious activity.

For example, in a typical third-party payment processor relationship, the payment processor is a deposit customer of the financial institution which uses its deposit account to process payments for its merchant clients. The payment processor receives lists of payments to be generated by the merchant clients for the payment of goods or services and initiates the payments by creating and depositing them into a transaction account at a financial institution. In some cases, the payment processor may establish individual accounts at the financial institution in the name

[1] Financial Institution Letter (FIL) 127-2008, *Guidance on Payment Processor Relationships,* dated November 7, 2008. See: http://www.fdic.gov/news/news/financial/2008/fil08127.html.

Third-Party Payment Processors

continued from pg. 3

of each merchant client and deposit the appropriate payments into these accounts. The merchant may then be a co-owner of the deposit account and make withdrawals from the account to receive its sales proceeds, or the payment processor may periodically forward the sales proceeds from the account to the merchant. Alternatively, the payment processor may commingle payments originated by the merchant clients into a single deposit account in the name of the payment processor. In this case, the payment processor should maintain records to allocate the deposit account balance among the merchant clients.

Payment Types Used by Third-Party Payment Processors

Payment processors may offer merchants a variety of alternatives for accepting payments including credit and debit card transactions, traditional check acceptance, Automated Clearing House (ACH) debits and other alternative payment channels. The potential for misuse or fraud exists in all payment channels. However, the FDIC has observed that some of the most problematic activity occurs in the origination of ACH debits or the creation and deposit of remotely created checks.

Automated Clearing House Debits

The ACH network is a nationwide electronic payment network which enables participating financial institutions to distribute electronic credit and debit entries to bank accounts and settle these entries.

Common ACH credit transfers include the direct deposit of payroll and certain benefits payments. Direct debit transfers also may be made through the ACH network and include consumer payments for insurance premiums, mortgage loans, and other types of bills. Rules and regulations governing the ACH networks are established by NACHA - The Electronic Payments Association (formerly National Automated Clearing House Association)[2] and the Board of Governors of the Federal Reserve System.

Third-party payment processors initiate ACH debit transfers as payments for merchant clients by submitting these transfers, which contain the consumer's financial institution routing number and account number (found at the bottom of a check) to their financial institution to enter into the ACH networks. Telemarketers and online merchants obtain this information from the consumer and transmit it to the payment processor to initiate the ACH debit transfers. The risk of fraud arises when an illicit telemarketer or online merchant obtains the consumer's account information through coercion or deception and initiates an ACH debit transfer that may not be fully understood or authorized by the consumer.

As with all payment systems and mechanisms, the financial institution bears the responsibility of implementing an effective system of internal controls and ongoing account monitoring for the detection and resolution of fraudulent ACH transfers. If an unauthorized ACH debit is posted to a consumer's account, the procedures for resolving errors contained in the Federal Reserve Board's Regulation E,

[2] NACHA establishes the rules and procedures governing the exchange of automated clearinghouse payments. See http://www.nacha.org/c/achrules.cfm.

which governs electronic funds transfers,[3] provide the consumer 60 days after the financial institution sends an account statement to report the unauthorized ACH debit.[4] Regulation E requires the consumer's financial institution to investigate the matter and report to the consumer the results of the investigation within a prescribed time frame. In the case of an ACH debit, when a consumer receives a refund for an unauthorized debit, ACH rules permit the consumer's financial institution to recover the amount of the unauthorized payment by returning the debit item to the originating financial institution.

Remotely Created Checks

Remotely Created Checks (RCCs), often referred to as "demand drafts," are payment instruments that do not bear the signature of a person on whose account the payments are drawn. In place of the signature, the RCC bears the account holder's printed or typed name, or a statement that the accountholder's signature is not required or the account holder has authorized the issuance of the check. Similar to the initiation of an ACH debit transfer, an account holder authorizes the creation of an RCC by providing his financial institution's routing number and his account number. Examples of RCCs are those created by a credit card or utility company to make a payment on an account, or those initiated by telemarketers or online merchants to purchase goods or services.

The risk of fraud associated with RCCs is often greater than the risk associated with other kinds of debits that post to transaction accounts. For example, an illicit payment originator might obtain a consumer's account information by copying it from an authorized check or misleading the consumer into providing the information over the telephone or the Internet. Once the necessary information is obtained, the payment originator can generate unauthorized RCCs and forward them for processing. Similar to the responsibilities associated with the ACH network, the financial institution should implement an effective system of internal controls and account monitoring to identify and resolve the unauthorized RCC.

RCCs may be processed as a paper item through the customary clearing networks or converted to and processed as an ACH debit. However, check clearing and ACH rules differ as to the re-crediting of an accountholder for an unauthorized RCC and how losses are allocated by and between the participating financial institutions. RCCs processed as checks are governed by provisions of the Uniform Commercial Code (UCC) and the Expedited Funds Availability Act,[5] as implemented by Regulation CC. RCCs converted to ACH debits are governed by applicable ACH rules, the Electronic Fund Transfer Act, and Regulation E.

In response to heightened concern about the risk of fraud, in 2005 the Federal Reserve amended Regulation CC to transfer the liability for losses

[3] Provisions of the Federal Reserve Board's Regulation E establish the rights, liabilities, and responsibilities of participants in electronic fund transfer systems, such as automated teller machine transfers, telephone bill-payment services, point-of-sale terminal transfers, and preauthorized transfers from or to a consumer's account.

[4] 12 CFR Section 205.11.

[5] The Expedited Funds Availability Act (EFAA), enacted in 1987, addresses the issue of delayed availability of funds by banks. The EFAA requires banks to (1) make funds deposited in transaction accounts available to customers within specified time frames, (2) pay interest on interest-bearing transaction accounts not later than the day the bank receives credit, and (3) disclose funds-availability policies to customers.

Third-Party Payment Processors

continued from pg. 5

resulting from unauthorized RCCs.[6] At the same time, the Board also amended Regulation J (the Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire) to clarify that certain warranties, similar to those provided under the UCC, apply to RCCs collected through the Reserve Banks. In conjunction with Regulation CC, the amendments to Regulation J shifted the liability for losses attributed to unauthorized RCCs to the financial institution where the check is first deposited as this institution is in the best position to know its customer (the creator of the RCC) and determine the legitimacy of the deposits. The liability also creates an economic incentive for depository institutions to perform enhanced due diligence on those customers depositing RCCs. Furthermore, by providing the paying financial institution with the ability to recover against the financial institution presenting the unauthorized RCC, these regulatory changes should make it easier for customers to obtain re-credits.[7]

Types of High Risk Payments

Although many clients of payment processors are reputable merchants, an increasing number are not and should be considered "high risk." These disreputable merchants use payment processors to charge consumers for questionable or fraudulent goods and services. Often a disreputable merchant will engage in high pressure and deceptive sales tactics, such as aggressive telemarketing or enticing and misleading pop-up advertisements on Web sites. For example, consumers should be cautious when Web sites offer "free" information and ask consumers to provide payment information to cover a small shipping and handling fee. In some instances and without proper disclosure, consumers who agreed to pay these fees, often found their bank accounts debited for more than the fee and enrolled in costly plans without their full understanding and consent.[8] Still other disreputable merchants will use processors to initiate payments for the sale of products and services, including, but not limited to, unlawful Internet gambling and the illegal sale of tobacco products on the Internet.

Generally, high-risk transactions occur when the consumer does not have a familiarity with the merchant, or when the quality of the goods and services being sold is uncertain. Activities involving purchases made over the telephone or on the Internet tend to be riskier in that the consumer cannot fully examine or evaluate the product or service purchased. Similarly, the consumer may not be able to verify the identity or legitimacy of the person or organization making the sale.

[6] Effective July 1, 2006 [70 Fed. Reg. 71218-71226 (November 28, 2005)].

[7] Changes to Federal Reserve Bank Operating Circular No. 3 on the Collection of Cash Items and Returned Checks clarifies that 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), www.frbservices.org/files/regulations/pdf/operating_circular_3.pdf.

[8] Rules governing the use of telemarketing require verifiable authorization of payment for services. See the Federal Trade Commission Telemarketing Sales Rule [16 CFR 310]. See: http://www.ftc.gov/os/2002/12/tsrfinalrule.pdf.

Of particular concern, the FDIC and other federal regulators have seen an increase in payment processors initiating payment for online gaming activities that may be illegal. The Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) prohibits financial institutions from accepting payments from any person engaged in the business of betting or wagering with a business in unlawful Internet gambling (see the FDIC's Financial Institution Letter on the *Unlawful Internet Gambling Enforcement Act,* FIL-35-2010, dated June 30, 2010).[9]

High-Risk Payment Processor Relationship Warning Signs

Financial institutions and examiners should be aware of the warning signs that may indicate heightened risk in a payment processor relationship. One of the more telling signs is a high volume of consumer complaints that suggest a merchant client is inappropriately obtaining personal account information; misleading customers as to the quality, effectiveness, and usefulness of the goods or services being offered; or misstating the sales price or charging additional and sometimes recurring fees that are not accurately disclosed or properly authorized during the sales transaction. However, this may be somewhat difficult to determine in that it may be almost

[9] 12 CFR Part 233 – Regulation GG, Financial Institution Letter (FIL) 35-2010, *Unlawful Internet Gambling Enforcement Act,* dated June 30, 2010. See http://www.fdic.gov/news/news/financial/2010/fil10035.html.

Third-Party Payment Processors

continued from pg. 7

impossible for financial institutions and examiners to know if consumers are submitting complaints directly to the payment processor or the merchants. One way financial institutions and examiners can determine if consumers are making complaints or voicing their dissatisfaction is to review certain Web sites, such as those for regional Better Business Bureaus, or blogs intended to collect and share such information to alert other consumers.

Financial institutions with third-party payment processor relationships should consider monitoring the Internet for complaints that mention them by name. The financial institution's name typically appears on the face of a RCC or in the record of an ACH debit. As a result, consumers often associate the financial institution with the transaction and may complain about the institution facilitating the payment. Complaints also may be lodged with the depository financial institution by the financial institution of the consumer whose account was charged. As required by statute and federal regulation, the depository financial institution must acknowledge, research, and respond to each complaint made directly to them.

Another indication of the potential for heightened risk in a payment processor relationship is a large number of returns or charge backs. Consumers who are dissatisfied with goods or services delivered or provided, or consumers who feel they were deceived or coerced into providing their account information, can request their financial institution return the RCC or ACH debit to the depository financial institution as an unauthorized transaction. In addition, items may be returned if insufficient funds are available to cover the unauthorized items, resulting in the consumer's account being overdrawn. In these circumstances, the items often are returned as "NSF" rather than as "unauthorized." Accordingly, financial institutions with payment processor relationships should implement systems to monitor for higher rates of returns or charge backs, which can be evidence of fraudulent activity.

Another warning sign is a significant amount of activity which generates a higher than normal level of fee income. In an increasingly competitive market place, financial institutions are looking for ways to grow non-interest fee income, and this is especially true for troubled institutions. Although fee income from third-party payment processor relationships may benefit an institution's bottom line, it can indicate an increased level of risk. Side agreements may be established between payment processors and financial institutions, whereby the payment processor pays the institution a fee for each item deposited, generating a higher level of fee income. However, the greatest source of income from these relationships tends to be returned item fees. Financial institutions routinely charge deposit customers a fee for each returned item. Because payment processors may generate a high volume of returned items, the fee income associated with this activity is typically much higher.

As a caveat, financial institutions and examiners should be alert for payment processors that use more than one financial institution to process merchant client payments, or nested arrangements where a payment processor's merchant client is also doing third-party payment processing. Spreading the activity among several institutions may allow processors that engage in inappropriate activity to avoid detection. For example, a single institution may not detect high levels of returned items if they are spread among several financial institutions.

Payment processors also may use multiple financial institutions in case one or more of the relationships is terminated as a result of suspicious activity.

Finally, another troubling development is payment processors that purposefully solicit business relationships with troubled institutions in need of capital. Payment processors identify and establish relationships with troubled institutions as these institutions may be more willing to engage in higher-risk transactions in return for increased fee income. In some cases, payment processors have made a commitment to purchase stock in certain troubled financial institutions or guarantee to retain a large deposit with the institution, thereby providing additional, 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.

Risk Controls

A framework for prudently managing relationships with third-party payment processors was communicated in the FDIC's 2008 *Guidance on Payment Processor Relationships.*[10] Financial institutions in relationships with payment processors should establish clear lines of responsibility for controlling the associated risks. Such responsibilities include effective due diligence and underwriting, as well as ongoing monitoring of high-risk accounts for an increase in unauthorized returns and suspicious activity and maintenance of adequate balances or reserves to cover expected high levels of returned items. The relationship should be governed by a written contract between the financial institution and the third-party payment processor which outlines each party's duties and responsibilities. Implementing appropriate and effective controls over payment processors and their merchant clients will help identify those processors working with fraudulent telemarketers or other unscrupulous merchants and help ensure the financial institution does not facilitate such transactions.

Due Diligence and Underwriting

Due diligence and prudent underwriting standards are critical components of a risk mitigation program. Financial institutions should implement policies and procedures that reduce the likelihood of establishing or maintaining a relationship with payment processors 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 incorporate an effective due diligence and underwriting policy that, among other things, requires background checks of payment processors and merchant clients. A processor approval program will help validate the activities, creditworthiness, and business practices of the payment processor and should, at a minimum,

[10] Financial Institution Letter (FIL) 127-2008, *Guidance on Payment Processor Relationships,* November 7, 2008, http://www.fdic.gov/news/news/financial/2008/fil08127.html.

Third-Party Payment Processors

continued from pg. 9

authenticate the processor's business operations and assess the entity's risk level. Any processor assessment should include:

- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele.
- Determining if the processor re-sells its services to "Independent Sales Organizations" (companies contracted to procure new merchant relationships) or through "gateway arrangements" (selling excess capacity to third parties, which in turn sell services to other individuals unknown to the payment processor).
- 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.
- Determining whether the institution maintains appropriate balances or reserves for each individual merchant based on the type of client and the risk involved in the transactions processed and the expected volume of returned items.
- Reviewing corporate documentation, obtaining information on the processor from independent reporting services and, if applicable, documentation on principal owners.
- Visiting the processor's business operations center.
- Requesting copies of consumer complaints and the procedures for handling consumer complaints and redress.
- Obtaining information pertaining to any litigation and actions brought by federal, state, or local regulatory or enforcement agencies.
- Obtaining information about the history of returned items and customer refunds.

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. 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 credit report from a consumer reporting agency or the state Better Business Bureau, or checking references from other financial institutions.

Ongoing Monitoring

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.[11] However, 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 Federal Financial Institutions Examination Council BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk with respect to 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.[12]

Appropriate Supervisory Responses

In those instances where examiners determine that a financial institution fails to have an adequate program in place to monitor and address risks associated with third-party payment processor relationships, formal or informal enforcement actions may be appropriate. Formal actions have included Cease and Desist Orders under Section 8(b) or 8(c) of the *Federal Deposit Insurance (FDI) Act*, as well as assessment of Civil Money Penalties under Section 8(i) of the FDI Act. These orders have required the financial institution to immediately terminate the high-risk relationship and establish reserves or funds on deposit to cover anticipated charge backs.

As appropriate, the examiner will determine if financial institution management has knowledge that the payment processor or the merchant clients are engaging in unfair or deceptive practices in violation of Section 5 of the Federal Trade Commission Act. In those cases where a financial institution does not conduct due diligence, accepts a heightened level of risk, and allows transactions for high-risk merchants to pass though it, it may be determined that the financial institution is aiding and abetting the merchants. This also could indicate a disregard for the potential for financial harm to consumers and, as a result, the financial institution may be subject to civil money penalties or required to provide restitution.

[11] Banks, bank holding companies, and their subsidiaries are required by federal regulations to file a Suspicious Activity Report if they know, suspect, or have reason to suspect the transaction may involve potential money laundering or other illegal activity, is designed to evade the Bank Secrecy Act or its implementing regulations, has no business or apparent lawful purpose, or is not the type of transaction in which particular customer would normally be expected to engage. See 12 CFR 353 (http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/12CFR353.htm) and 31 CFR 103.18 (http://www.ffiec.gov/bsa_aml_infobase/pages_manual/regulations/31CFR103.pdf.)

[12] See "Third-Party Payment Processors—Overview," from the Bank Secrecy Act/Anti-Money Laundering Examination Manual, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm.

Third-Party Payment Processors

continued from pg. 11

Conclusion

Deposit relationships with payment processors expose financial institutions to risks that may not be present in relationships with other commercial customers. To limit potential risks, financial institutions should implement risk mitigation policies and procedures that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, risk mitigation programs should result in the financial institution assessing its risk tolerance for this type of activity, verifying the legitimacy of the payment processor's business operations, and monitoring payment processor relationships for suspicious activity.

Financial institutions should act promptly if they believe fraudulent or improper activities have occurred related to a payment processor's activities. Appropriate actions may include 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. Should it be determined that a financial institution does not have an adequate program in place to monitor and address the risks associated with third-party payment processor relationships, an appropriate supervisory response will be used to require the financial institution to correct the deficiencies.

Michael B. Benardo
Chief, Cyber-Fraud and Financial Crimes Section
Division of Risk Management Supervision
mbenardo@fdic.gov

Kathryn M. Weatherby
Examination Specialist (Fraud)
Cyber-Fraud and Financial Crimes Section
Division of Risk Management Supervision
kweatherby@fdic.gov

Robert J. Wirtz
Assistant Regional Director (Compliance)
Division of Depositor and Consumer Protection
rwirtz@fdic.gov