Third-Party Payment Processors — Overview

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with its relationships with third-party payment processors, and management's ability to implement effective monitoring and reporting systems.*

Nonbank or third-party payment processors (processors) are bank customers that provide payment-processing services to merchants and other business entities. Traditionally, processors contracted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house (ACH) transactions,[221] remotely created checks (RCC),[222] and debit and prepaid cards transactions. With the expansion of the Internet, retail borders have been eliminated. Processors now provide services to a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, telemarketers, and Internet gaming enterprises.

Third-party payment processors often use their commercial bank accounts to conduct payment processing for their merchant clients. For example, the processor may deposit into its account RCCs generated on behalf of a merchant client, or process ACH transactions on behalf of a merchant client. In either case, the bank does not have a direct relationship with the merchant. The increased use of RCCs by processor customers also raises the risk of fraudulent payments being processed through the processor's bank account. The Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Financial Crimes Enforcement Network (FinCEN) have issued guidance regarding the risks, including the BSA/AML risks, associated with banking third-party processors.[223]

Risk Factors

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, or other illicit transactions, including those prohibited by OFAC.

The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which the bank's customer conducts transactions through the bank on

[221] NACHA – The Electronic Payments Association (NACHA) is the administrator of the Automated Clearing House (ACH) Network. The ACH Network is governed by the NACHA Operating Rules, which provides the legal foundation for the exchange of ACH and IAT payments. The NACHA Web site includes additional information about the ACH payment system.

[222] A remotely created check (sometimes called a "demand draft") is a check that is not created by the paying bank (often created by a payee or its service provider), drawn on a customer's bank account. The check often is authorized by the customer remotely, by telephone or online, and, therefore, does not bear the customer's handwritten signature.

[223] *FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors*, FDIC FIL-41-2014, July 28, 2014; *Payment Processor Relationships Revised Guidance*, FDIC FIL-3-2012, January 31, 2012; *Risk Management Guidance: Payment Processors*, OCC Bulletin 2008-12, April 24, 2008; *Risk Management Guidance: Third Party Relationships*, OCC Bulletin 2013-29, October 30, 2013; and *Risk Associated with Third-Party Payment Processors*, FinCEN Advisory FIN-2012-A010, October 22, 2012.

behalf of the customer's clients. When the bank is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. If a bank has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or OFAC-sanctioned transactions.

While payment processors generally affect legitimate payment transactions for reputable merchants, the risk profile of such entities can vary significantly depending on the make-up of their customer base. Banks with third-party payment processor customers should be aware of the heightened risk of returns and use of services by higher-risk merchants. Some higher-risk merchants routinely use third parties to process their transactions because they do not have a direct bank relationship. 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. Risks are heightened when the processor does not perform adequate due diligence on the merchants for which they are originating payments.

Risk Mitigation

Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. A bank may assess the risks associated with payment processors by considering the following:

- Implementing a policy that requires an initial background check of the processor (using, for example, the Federal Trade Commission Web site, Better Business Bureau, Nationwide Multi-State Licensing System & Registry (NMLS), NACHA, state incorporation departments, Internet searches, and other investigative processes), its principal owners, and of the processor's underlying merchants, on a risk-adjusted basis in order to verify their creditworthiness and general business practices.
- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele. A bank may develop policies, procedures, and processes that restrict the types of entities for which it allows processing services. These restrictions should be clearly communicated to the processor at account opening.
- Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.[224]
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.

[224] Gateway arrangements are similar to an Internet service provider with excess computer storage capacity that sells its capacity to a third party that would then distribute computer services to various other individuals unknown to the provider. The third party would be making decisions about who would be receiving the service, although the provider would be providing the ultimate storage capacity. Thus, the provider bears all of the risks while receiving a smaller profit.

- Requiring the processor to identify its major customers by providing information such as the merchant's name, principal business activity, geographic location, and transaction volume.
- Verifying directly, or through the processor, that the merchant is operating a legitimate business by comparing the merchant's identifying information against public record databases, and fraud and bank check databases.
- Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- 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.

Banks that provide account services to third-party payment processors should monitor their processor relationships for any significant changes in the processor's business strategies that may affect their risk profile. Banks should periodically re-verify and update the processors' profiles to ensure the risk assessment is appropriate. Banks should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. Banks should periodically audit 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.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. To effectively monitor these accounts, the bank should have an understanding of the following processor information:

- Merchant base.
- Merchant activities.
- Average dollar volume and number of transactions.
- "Swiping" versus "keying" volume for credit card transactions.
- Charge-back history, including rates of return for ACH debit transactions and RCCs.
- Consumer complaints or other documentation that suggest a payment processor's merchant clients are inappropriately obtaining personal account information and using it to create unauthorized RCCs or ACH debits.

With respect to account monitoring, a bank should thoroughly investigate high levels of returns and should not accept high levels of returns on the basis that the processor has provided collateral or other security to the bank. High levels of RCCs or ACH debits returned for insufficient funds or as unauthorized can be an indication of fraud or suspicious activity. Therefore, return rate monitoring should not be limited to only unauthorized transactions, but include returns for other reasons that may warrant further review, such as unusually high rates of return for insufficient funds or other administrative reasons.

Transactions should be monitored for patterns that may be indicative of attempts to evade NACHA limitations on returned entries. For example, resubmitting a transaction under a different name or for slightly modified dollar amounts can be an attempt to circumvent these limitations and are violations of the NACHA Rules. [225]

A bank should implement appropriate policies, procedures, and processes that address compliance and fraud risks. Policies and procedures should outline the bank's thresholds for returns and establish processes to mitigate risk from payment processors, as well as possible actions that can be taken against the payment processors that exceed these standards.

If the bank determines a SAR is warranted, FinCEN has requested banks check the appropriate box on the SAR report to indicate the type of suspicious activity, and include the term "payment processor," in both the narrative and the subject occupation portions of the SAR.

[225] Refer to NACHA Operating Rules.