STAY CURRENT
A Client Alert from Paul Hastings

PAUL HASTINGS

February 2012

FDIC Updates Guidance on Payment Processor Relationships

BY KEVIN L. PETRASIC

In its recently issued Financial Institution Letter, FIL-3-2012, the Federal Deposit Insurance Corporation ("FDIC") updated the agency's November 2008 guidance on the potential risks to insured depository institutions of payment processor relationships.[1] The updated guidance is in response to the increased number of deposit relationships between insured institutions and payment processors utilizing institutions' deposit accounts to process payments for third-party merchants and, in some cases, other payment processors.

The FDIC guidance addresses bank relationships with companies that process payments for a wide variety of entities, including telemarketers, online businesses, and other types of merchants. A particular emphasis of the newly issued guidance relates to FDIC expectations regarding how institutions should be monitoring and mitigating risks arising from these relationships, as well as due diligence efforts necessary to understand the underlying risks related to payment processor relationships with merchants, as well as other payment processors that a processor may service.

While focused on depository institution payment processor relationships, FIL-3-2012 highlights a number of important regulatory and supervisory issues presented by the intersection of traditional bank products and services with rapidly evolving payment systems practices and technologies, including card-based, internet and electronic funds transfers, and other emerging e-commerce and mobile payment systems products and services. The FDIC guidance presents important insights for insured institutions with respect to a wide variety of third-party relationship management issues. These issues are important to insured institutions, entities that utilize institution products and services in dealing with third parties, and vendors providing or managing third-party relationship products and services for or through insured institutions.

Overview

As noted in the FDIC's guidance, payment processors typically process payments either by creating and depositing remotely created checks ("RCCs"), also known as "demand drafts," or by originating Automated Clearing House ("ACH") debits on behalf of merchant customers. Payment processors may use their own deposit account to process such transactions, or may establish separate deposit accounts for their merchant clients in order to process the transactions.

The FDIC guidance highlights the following important considerations for depository institutions maintaining or establishing payment processor relationships:

- Institutions should conduct careful due diligence and prudent underwriting in establishing, and careful monitoring in maintaining, account relationships with third-party payment processors;
- Institutions should pay particular attention to account relationships with high-risk entities that could expose the institution to risks arising from unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act;
- Institutions should carefully review and monitor heightened money laundering and fraud risks that may exist with payment processors that fail to verify merchant client identities and monitor customer merchant business practices;
- Institutions should monitor and review consumer complaints or unusual return rates that may indicate the inappropriate use of personal account information and possible deception or unfair treatment of consumers;
- Institutions should have policies in place promptly to address fraudulent or improper activities involving payment processor relationships; and
- Institutions failing to manage risks arising from payment processor relationships may be subject to various enforcement actions, including civil money penalties and restitution orders.

Know Your Payment Processor

Perhaps the most important message in the FDIC's newly issued guidance is the need for insured institutions to know and understand the risks presented by an individual payment processor relationship, including the payment processor's processes for verifying the identity of its merchant customers and their business operations and practices. Institutions that fail to implement adequate controls to understand and manage third-party risks arising from a payment processor relationship expose the institution to elevated money laundering and fraud risk, along with legal, reputational, and compliance risks if consumers are harmed. To manage the risks, insured institutions must understand, verify, and monitor the activities and the entities related to each account relationship, particularly given the absence of a direct customer relationship with merchant clients of the payment processor.

Managing the Payment Processor Relationship

> *"Deposit relationships with payment processors expose institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks."*

Certainly, an important aspect of managing a payment processor relationship is the contractual agreement that forms the basis of the relationship. At a minimum, contracts with payment processors must provide a depository institution with "access to necessary information in a timely manner." In addition, a contract should provide for immediate termination of the relationship where a processor exposes the institution to undue risks, as well as establishing an adequate reserve requirement to cover anticipated charge-backs. In managing payment processor relationship risks, insured institutions are expected to oversee all transactions and processing activities, as well as to manage and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks arising from the relationship.

> *"Insured institutions should also 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."*

An important point stressed in the FDIC guidance is the potential liability to institutions that fail to

adequately manage payment processor relationships and, as a result, may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity. A particular concern is potential liability for "facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act."

Several additional issues highlighted by the FDIC include risks posed by payment processors that use multiple financial institutions to process merchant client payments, and payment processors that solicit business relationships with troubled depository institutions. In both cases, payment processors may be engaging in opportunistic activities that are not serving the best interests of the insured institution. Particularly vulnerable targets include smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

In managing payment processor relationships, institutions should also monitor consumer complaint activity, including complaints received at the institution, complaint activity at a payment processor or with its underlying merchants, and other independent sources of complaint data or other investigations or legal action. When identifying problems, institutions are expected to act promptly to address possible consumer harm. Where potentially fraudulent or improper activities are involved, appropriate responses include filing a Suspicious Activity Report and taking directed action against a payment processor and/or merchant, such as suspending or terminating the relationship or freezing an account to cover future charge-backs.

Internal Risk Controls

An important aspect of effectively managing a payment processor relationship is implementing and maintaining internal controls to mitigate risk. Appropriate and well-defined controls 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."[2] Effective controls will help in avoiding risky payment processor relationships, as well as in detecting and minimizing risks arising from fraudulent merchant activities in existing relationships.

A. *Establishing the Relationship*

Financial institutions are expected to implement policies and procedures designed to avoid risky payment processor relationships. Institutions should have clearly articulated thresholds for unauthorized returns, a strong due diligence and underwriting policy for screening new payment processors, including understanding the nature of the business operations and existing merchant relationships, and a method for authenticating the operations and assessing the underlying merchant risks. Relevant factors include:

- Identifying a processor's major lines of business and merchant customer volume;
- Reviewing a processor's due diligence standards for new merchants;
- Reviewing corporate documentation and external information on principal owners and operators;
- Conducting an on-site review of a processor's business operations;
- Reviewing a processor's promotional materials to determine target clients;
- Reviewing "gateway arrangements" where a processor re-sells its services to a third party;
- Assessing potential conflicts of interest that exist between processor management and institution insiders;

- Assessing the adequacy and verification of information on a processor's merchant clients and merchants' affiliates; and
- Conducting independent operational audits on a payment processor calibrated to the degree to which the institution will rely on the processor for merchant client due diligence.

B. *Maintaining the Relationship*

The FDIC guidance notes that an important aspect of managing risk in an existing payment processor relationship is monitoring transaction activity for higher rates of returns or charge backs and/or high levels of returns arising from unauthorized RCCs or ACH debits. All of these circumstances can be indicative of fraudulent activity. An equally important and often more difficult issue involves BSA/AML compliance. While institutions are required to implement comprehensive compliance programs, the FDIC guidance notes that "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." Thus, institutions maintaining payment processor relationships should have procedures in place to monitor transaction activity, volume, merchant data, and charge-back history.

> *"Consumer complaints and/or high rates of return may be an indicator of unauthorized or illegal activity."*

Institutions should also regularly screen consumer complaint activity at a payment processor and its merchant clients. This will enable institutions to identify and detect risks related to fraud and/or illegal activity. In this regard, institutions should have formalized procedures for routine audits of third-party payment processing relationships. Such audits should review merchant client relationships and processors' contractual obligations to merchants that may impact the institution.

Action Plan – Establish and Maintain Effective Risk Mitigation Techniques

A critical aspect of an insured institution's payment processor program is establishing and maintaining effective oversight and controls to minimize potential risks arising from such relationships. Key issues for an effective program are assessing risk tolerance, verifying a payment processor's business operations, evaluating ownership and control, and establishing ongoing monitoring of account relationships. Equally important are institution policies and procedures for detecting and addressing fraudulent or improper activities, and for avoiding and addressing consumer harm.

As with any activity involving third-party arrangements, institutions should pay close attention not only to their own internal monitoring and controls, but also to those of the payment processors in which they establish and maintain an account relationship. In assessing risks posed by payment processor relationships, institutions must understand the unique business operations of each payment processor relationship, as well as the relationships that each payment processor has with each of its merchant clients. This requires a coordinated compliance program in which the institution and payment processor must partner to minimize operational risks and avoid supervisory scrutiny.

Institutions should review their existing policies and procedures both for establishing payment processor relationships and maintaining such relationships. Internal risk controls should be calibrated based on the particular circumstances of each payment processor relationship (including the nature of the processor's underlying merchant clientele) and institutions should be particularly mindful of maintaining contractual rights, terms, and conditions that provide remedies to address potential problems. These include invoking appropriate institution responses to address potentially fraudulent or improper activities, such as filing Suspicious Activity Reports, where appropriate, and taking directed

action against a payment processor and/or merchant, including suspending or terminating a relationship or freezing an account to cover future anticipated charge-backs.

Paul Hastings lawyers are actively working with insured institution and payment processor clients to identify and address issues and risks related to payment processor relationships, including developing and implementing risk mitigation policies and programs for institutions and processors to establish and maintain effective, safe, and profitable payment processor programs.

✧ ✧ ✧

If you have any questions regarding the FDIC's recently issued payment processor guidance, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Chris Daniel
1.404.815.2217
chrisdaniel@paulhastings.com

Todd W. Beauchamp
1.404.815.2154
toddbeauchamp@paulhastings.com

Kevin Erwin
1.404.815.2312
kevinerwin@paulhastings.com

Diane Pettit
1.404.815.2326
dianepettit@paulhastings.com

Palo Alto

Cathy S. Beyda
1.650.320.1824
cathybeyda@paulhastings.com

San Francisco

Thomas Brown
1.415.856.7248
tombrown@paulhastings.com

Stanton R. Koppel
1.415.856.7284
stankoppel@paulhastings.com

Washington, DC

V. Gerard Comizio
1.202.551.1272
vgerardcomizio@paulhastings.com

Kevin L. Petrasic
1.202.551.1896
kevinpetrasic@paulhastings.com

Erica Berg-Brennan
1.404.815.2294
ericaberg@paulhastings.com

Lawrence D. Kaplan
1.202.551.1829
lawrencekaplan@paulhastings.com

Michael Hertzberg
1.202.551.1797
michaelhertzberg@paulhastings.com

Helen Y. Lee
1.202.551.1817
helenlee@paulhastings.com

Scott Lieberman
1.202.551.1751
scottlieberman@paulhastings.com

Amanda M. Jabour
1.202.551.0376
amandajabour@paulhastings.com

[1] FDIC Financial Institution Letter FIL-3-2012, "Payment Processor Relationships: Revised Guidance" (January 31, 2012).
[2] *Id.* at 3.