Paul Hastings
StayCurrent
A CLIENT ALERT FROM PAUL HASTINGS
December 2008

Recent FDIC Guidance on Providing Banking Services to Payment Processors or How to Avoid Engaging in "Rent-A-Bin" Relationships

BY CHRIS DANIEL AND TODD BEAUCHAMP

I. Introduction

The Federal Deposit Insurance Corporation ("FDIC") recently issued Financial Institution Letter 127-2008, which provides guidance to financial institutions regarding due diligence measures that they should undertake in screening payment processors as potential customers, as well as the steps that institutions should take as part of their ongoing monitoring of such customers' activities. The focus of this guidance is on relationships with payment processors that create and deposit Remotely Created Checks ("RCCs"), as well as originate Automated Clearing House ("ACH") debits on behalf of their merchant customers. These activities can present significant money laundering and fraud risks, which are heightened where the processor does not conduct appropriate due diligence on the merchants for whom it originates the payments.

This release follows the action taken by the Office of the Comptroller of Currency ("OCC") against Wachovia Bank, N.A. in April 2008, and generally mirrors OCC Bulletin 2008-12 that was issued later that same month. In the Wachovia action, the OCC assessed Wachovia for penalties totaling roughly $149 million (comprised of amounts to repay affected accountholders, civil money penalties, and amounts to pay for consumer education programs) as a result of the fraudulent use of RCCs by telemarketers and payment processors that maintained account relationships with the bank. This action emphasizes the need for banks to be diligent in verifying the legitimacy of not only the business activities of their customers acting as third-party senders, but also the activities of the merchants and telemarketers for whom the third-party sender is processing transactions, as banks that do not may be viewed as facilitating the fraudulent or unlawful activity by the customer or its merchant client.

II. Summary

The release sets forth the following measures, which are substantially similar to the obligations that all financial institutions have with respect to screening and monitoring their third-party service providers.

A. Due Diligence and Underwriting

Each financial institution that initiates transactions for payment processors should ensure that its customer approval program provides for an assessment of the processor's business operations and risk level, as well as a review of information relating to each of the processor's merchant clients. For each processor, the institution should:

- Review the processor's promotional materials, including its website, to determine the target clientele;
- Determine 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";
- Review the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants;
- Identify the major lines of business and volume for the processor's customers;
- Review corporate documentation, including information from independent reporting services and, if applicable, documentation on principal owners;
- Visit the processor's business operations center.

Furthermore, the institution should require each processor to provide background information on each of its merchant clients, such as the merchant's name, principal business activity, geographic location, and sales techniques, as well as verify directly, or through the processor, that the merchant is operating a legitimate business, possibly by obtaining a credit report or checking other financial institution references. Finally, each institution should ensure that payment processors engaged in the creation of remotely created checks, as well as their merchant clients, comply with the regulatory framework applicable to such instruments and have a process in place to remain informed of changes in applicable law.

B. Ongoing Monitoring

Institutions are encouraged to implement systems designed to detect high levels of ACH debits or remotely created checks that are returned as unauthorized or due to insufficient funds, as this can indicate the presence of fraudulent activity. Additionally, institutions should ensure that their risk management programs provide for ongoing review of the transaction volume and charge-back history associated with each payment processor in order to detect suspicious activity.

III. Conclusion

It is, of course, entirely appropriate for federally insured financial institutions to provide payment system and account services to payment processors, the vast majority of which operate within the law and apply appropriate underwriting criteria to their own clients. However, a depository institution does incur heightened risk when it (a) provides payment system and account services to a payment processor, and (b) the depository institution does not have a direct relationship with the clients of the payment processor itself. It has been our experience that the federal banking agencies are looking much more closely at bank/payment processor and bank/third-party service provider relationships to ensure that such relationships do not pose an undue risk to the depository institution or that the depository institution is not being used as an unwitting accomplice in fraudulent transactions or transactions or products which may be perceived as being in violation of the Federal Trade Commission Act (see, for example, the OCC's action against Wachovia discussed above and the FDIC's action against CompuCredit and two other federally insured financial institutions announced in June of this year).

✧ ✧ ✧

The full text of FIL 127-2008 is available at: http://www.fdic.gov/news/news/financial/2008/fil08127a.html

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Atlanta lawyers:

Todd W. Beauchamp
404-815-2154
toddbeauchamp@paulhastings.com

Chris Daniel
404-815-2217
chrisdaniel@paulhastings.com

Stay*Current* is published solely for the interests of friends and clients of Paul, Hastings, Janofsky & Walker LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership.

IRS Circular 230 Disclosure: As required by U.S. Treasury Regulations governing tax practice, you are hereby advised that any written tax advice contained herein or attached was not written or intended to be used (and cannot be used) by any taxpayer for the purpose of avoiding penalties that may be imposed under the U.S. Internal Revenue Code.