Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2012-A010
Issued: October 22, 2012
Subject: Risk Associated with Third-Party Payment Processors

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to provide guidance to financial institutions when filing Suspicious Activity Reports (SARs) on activities related to third-party payment processors ("Payment Processors"). This Advisory furthers the Department of the Treasury's broader efforts to protect the U.S. financial system from money laundering and terrorist financing.

Description of Third-Party Payment Processors

Non-Bank, or third-party, Payment Processors are financial institution customers that provide payment processing services to merchants and other business entities, typically initiating transactions on behalf of merchant clients that do not have a direct relationship with the Payment Processor's financial institution. Payment Processors use their own deposit accounts at a financial institution to process such transactions and sometimes establish deposit accounts at the financial institution in the names of their merchant clients. Traditionally, Payment Processors contracted primarily with U.S. retailers that had physical locations in the United States in order to help collect monies owed by customers on the retailers' transactions. These merchant transactions primarily included credit card payments, but also covered Automated Clearing House (ACH) debits and creating and depositing remotely created checks (RCCs) or "demand drafts." With the expansion of the Internet, Payment Processors may now service a variety of domestic and international merchants, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.[1]

---

[1] *See* Federal Financial Institutions Examination Council (FFIEC) Exam Manual, pp. 239-242 (April 29, 2010). Although the FFIEC Exam Manual is issued by the federal banking regulators and relates to AML requirements applicable to banks, it contains guidance that may be of interest to all financial institutions that provide financial services to Payment Processors and MSBs.

Potential Red Flags for Illicit Use of Payment Processors[2]

Law enforcement has reported to FinCEN that recent increases in certain criminal activity have demonstrated that Payment Processors present a risk to the payment system by making it vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. Many Payment Processors provide legitimate payment transactions for reputable merchant clients. The risk profile of such entities, however, can vary significantly depending on the composition of their customer base. For example, Payment Processors providing consumer transactions on behalf of telemarketing and Internet merchants may present a higher risk profile to a financial institution than would other businesses. Telemarketing and Internet sales and RCC-related transactions tend to have relatively higher incidences of consumer fraud or potentially illegal activities.

Trends and indicators of suspicious activity associated with Payment Processors are provided by federal, state, and local law enforcement agencies, who work together under the Financial Fraud Enforcement Task Force's (FFETF) Consumer Protection Working Group. Suspicious activity as described below often is associated with Payment Processors engaged in improper or illegal conduct.

- *Fraud:* High numbers of consumer complaints about Payment Processors and/or merchant clients, and particularly high numbers of returns or charge backs (aggregate or otherwise), suggest that the originating merchant may be engaged in unfair or deceptive practices or fraud, including using consumers' account information to create unauthorized RCCs or ACH debits. Consumer complaints are often lodged with financial institutions, Payment Processors, merchant clients, consumer advocacy groups, online complaint Web sites or blogs, and governmental entities such as the Federal Trade Commission and state Attorneys General.

- *Accounts at Multiple Financial Institutions:* Payment Processors engaged in suspicious activity often maintain accounts at more than one financial institution. Similarly, they may move from one financial institution to another within a short period. Such Payment Processors also may use multiple financial institutions and maintain redundant banking relationships in recognition of the risk to the Payment Processor and merchant that a financial institution may recognize the suspicious activity and terminate the Payment Processor and/or merchant accounts. In addition, regulators and law enforcement have recognized an increased use of "check consolidation accounts"[3] by some Payment Processors.

---

[2] For additional information on fraudulent schemes identified by various government offices, refer to their websites and the DOJ FFETF site www.STOPFRAUD.GOV. Additional information on consumer fraud involving the use of Payment Processors and RCCs can be found at http://www.ftc.gov/.

[3] Returned Check Consolidation Accounts are legitimate and commonly used by commercial enterprises to facilitate processing of returned checks. Recently, however, some Payment Processors have used these accounts to establish separate deposit accounts to disposition their returned check items for the purpose of making it difficult for financial institutions to identify and evaluate "return/error" rates for the Payment Processor. In some instances, both the deposit account and the returned check consolidation account are held at the same institution but in different accounts. In other instances, the accounts are held at separate institutions. In either case, this account relationship structure severely inhibits a financial institution's ability to monitor and report suspicious activity.

Consolidation accounts can be used by Payment Processors to conceal high return or chargeback rates from originating financial institutions and regulators.

- *Money Laundering:* Criminals are continually looking for ways to launder illicit proceeds, including the proceeds of consumer fraud. Payment Processors can be used by criminals to mask illegal or suspicious transactions and to launder proceeds of crime. In addition, Payment Processors have been used to place illegal funds directly into a financial institution using ACH credit transactions originating from foreign sources.

- *Enhanced Risk:* There are potential risks associated with relationships with third-party entities, in particular foreign-located payment processors that process payments for telemarketers, online businesses, and other merchants. These relationships can pose increased risk to institutions and may require careful due diligence and monitoring.

- *Solicitation for Business:* Payment Processors engaged in suspicious activity have been known to solicit business relationships with distressed financial institutions in need of revenue and capital. Such Payment Processors may consider troubled financial institutions to be more willing to engage in higher-risk transactions. In some cases, Payment Processors also have committed to purchasing stock in these financial institutions to further induce the financial institution to provide banking services to high risk merchants. Often, the targeted financial institutions are smaller community banks that lack the infrastructure to properly manage or control a high-risk Payment Processor relationship. Fraudulent merchants also have been known to possess accounts through payment processors at large financial institutions.

- *Elevated rate of return of debit transactions due to unauthorized transactions:* Payment processors engaged in or complicit in suspicious activities may reflect a rate of return of debit items due to unauthorized transactions substantially higher than the average. Payment processors abused by criminals may show an acceptable rate (*i.e.* an average within normal parameters for the payment system involved) of returned items due to unauthorized transactions, calculated as a percentage of the processor's total transaction volume, but a much higher rate of returned items when the ratio is calculated on the traffic volume of individual originators.

Guidance

Financial institutions providing services to Payment Processors institutions may find it necessary to update their anti-money laundering programs.[4] Financial institutions should determine during thorough initial and ongoing due diligence, to the extent possible, whether external investigations or legal actions are pending against a Payment Processor or its owners and operators. Financial

---

[4] *See* footnote 1 above.

institutions also should determine whether Payment Processors have obtained all necessary state licenses, registrations, and approvals.[5]

Additionally, financial institutions may be required to file SARs if they know, suspect, or have reason to suspect that a Payment Processor has conducted a transaction involving funds derived from illegal activity, including, but not limited to, consumer fraud. A financial institution also may be required to file a SAR where it knows, suspects, or has reason to suspect that a Payment Processor has attempted to disguise funds derived from illegal activity, or has attempted to engage in transactions designed to evade regulations promulgated under the Bank Secrecy Act ("BSA") or that lack a legitimate business or apparent lawful purpose.[6]

To assist law enforcement in investigating and prosecuting possible criminal activity involving Payment Processors, FinCEN requests that, when reporting suspicious activity, financial institutions (1) check the appropriate box on the SAR form to indicate the type of suspicious activity, and (2) include the term "Payment Processor" in both the narrative portion and the subject occupation portions of the SAR.

Questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Regulatory Helpline at 800-949-2732. Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).

---

[5] Financial Crimes Enforcement Network, "Advisory – Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States," (April 26, 2005), *available at* http://www.fincen.gov/statutes_regs/guidance/html/guidance04262005.html.

[6] *See, e.g,.* 31 CFR § 1020.320.