November 2015

Managing TPPPs and TPSs in the Current Regulatory Environment

Prepared by:
Jodie Ruby, Director

Audience: This document is intended for managers, directors and executives who deal with business customer compliance and risk. In particular, this is intended for those who have working relationships or are seeking to establish working relationships with Third-Party Payment Processors and Third-Party Senders.

Table of Contents

Contents

Summary

Third-Party Payment Processors (TPPPs) and Third-Party Senders (TPSs) play an important role in the financial services industry, providing electronic payment services to numerous small to mid-sized businesses that otherwise would not have access to these services. Financial institutions can quickly grow their portfolios and boost their revenues by working with TPPPs*. However, given the lack of direct regulatory scrutiny placed on TPPPs, these companies are targets for money laundering, thus requiring closer investigation and monitoring by financial institutions. This white paper reviews the benefits and challenges of working with TPPPs, and the approach taken by a top financial institution to manage its TPPP portfolio that was well received by auditors and regulators.

*The term "TPPP" is used in this white paper as an umbrella term for third-party payment processors and third-party senders.

The Current Regulatory Environment

In the National Money Laundering Assessment updated in June 2015, the U.S. Department of the Treasury reviewed key money laundering and terrorist financing risks to the United States[1]. In this report, TPPPs are identified as posing a risk for money laundering, identity theft and fraud, because TPPPs are not bound by BSA/AML requirements as banks are. References are made to the FFIEC BSA/AML exam manual that highlights these risks, including the fact that risks increase when the processor lacks adequate due diligence of its merchant customers[2]:

> **FFIEC BSA/AML Examination Manual, p 236:**
>
> 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.

In addition to increased risks for money laundering, working with TPPPs introduces additional challenges for financial institutions including:

- **Compliance risk:** Financial institutions that work with TPPPs may find that these relationships expose them to a greater level of compliance risk resulting from the riskiness of a TPPP's underlying clients. There may be some TPPPs that deliver services to clients that engage in

deceptive, abusive or illegal practices, and institutions working with these TPPPs may be viewed as enabling these activities. Financial institutions that fail to adequately investigate and monitor TPPPs and their underlying customers may be subject to additional scrutiny from regulators, increased monitoring of their business customer portfolio and even substantial fines.

- **Reputational risk:** Decline in a customer's reputation can be a leading indicator of risk, yet this is often overlooked when managing business customer relationships on an ongoing basis. The CFPB has recently extended its scrutiny directly to TPPPs and has issued consent orders directly to processors who have failed to monitor their customers for declining reputation and customer complaints. A recent example of a consent order from August 2015 issued to Global Client Solutions highlights this trend. Global Client Solutions was fined $7 MM for assisting debt relief service providers in the collection of tens of millions of dollars in illegal upfront fees from consumers. Part of the consent order requires Global Client Solutions to obtain up to 200 of the most current consumer complaints about a debt relief service provider and any information regarding the resolution of the complaints[3]. As declining reputation is a leading indicator of risk, the CFPB requires this action be taken as part of the steps needed to remove the consent order.

- **Lack of transparency:** While working with TPPPs brings additional revenue to the financial institution, it also brings added complexity and reduces transparency. Regulators expect financial institutions to know their customer's customers (KYCC) which requires additional resources to manage. Lack of transparency into these customers can open up a financial institution to increased risks without the proper due diligence and monitoring.

- **Same Day ACH fraud risk:** With the move to Same Day ACH processing — which is anticipated to start September 2016 and will introduce two new payment submission windows — some predict that fraudsters may take advantage of the lack of transparency FIs have with TPPPs to submit fraudulent payments later in the day when analysts have less time to review submissions. This highlights the need to monitor TPPP relationships that much more closely[4].

While initial guidance from regulators as a result of Operation Choke Point prompted some financial institutions to cease doing business with entire categories of business customers — including TPPPs — regulators have since revised their guidance to state that banks should not de-risk entire classifications of customers, but rather should take a risk-based approach based on the risk appetite of their organization. According to Barbara Hagenbaugh*, deputy to the chairman for communications at the FDIC:*

> *"… the Federal Deposit Insurance Corp. encourages supervised institutions to take a risk-based approach in assessing customer relationships, rather than declining to provide banking services to entire categories of customers without regard to the risks presented by an individual customer or the financial institution's ability to manage the risk. That means that FDIC-supervised financial institutions that properly manage customer relationships and effectively mitigate risks are neither prohibited nor discouraged from providing services to any category of customer accounts or individual customers operating in compliance with applicable law.*[5]

Similarly, Michael Zeldin, former chief of money laundering at the DOJ, stated that:

> *"Derisking is really not and shouldn't be the complete elimination of classes of customers…One of the most significant problems is that banks just do not do their risk assessment as well and as*

granularly as they ought to. They focus instead on broad themes of products, services and geographies. They don't dial down into specifics of their customer base to understand what those risks are, how to mitigate those risks, and once you mitigate those risks, what are the appropriate fees to be charged for customers in that risk category." [6]

According to these experts, each business customer should be evaluated independently to determine if it fits the risk profile of the financial institution, rather than making decisions at the business category level.

A Case for Working with TPPPs

There are many benefits to establishing and maintaining TPPP relationships that financial institutions should consider. TPPPs provide electronic payments services to numerous companies — from startups to mid-sized — that otherwise would not have access to the financial system since they are deemed to be too small to have direct access through a bank. This opens up additional revenue streams for financial institutions, and the option to serve new verticals. With the TPPP as the intermediary, a financial institution can quickly scale to service many more customers in a shorter amount of time, while lowering its customer acquisition and servicing costs. As such, it reaps the financial rewards without having to hire additional staff to manage those direct customer relationships. With TPPPs as customers, a financial institution can cross-sell and upsell a variety of products to meet TPPP treasury management needs. All of this leads to more revenue for the financial institution.

As mentioned earlier, the current climate of de-risking as a result of Operation Choke Point has prompted many financial institutions to stop working with TPPPs. However, with the right due diligence and business customer monitoring tools in place, banks can establish business relationships with TPPPs with confidence, and establish themselves as preferred banks for these organizations.

How can financial institutions maintain their regulatory compliance when working with these potentially higher risk businesses? Again, the FFIEC examination manual provides guidance for risk mitigation:

FFIEC BSA/AML Examination Manual, p 236-237:

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 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.
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.
- Requiring the processor to identify its major customers by providing information such as the merchant's name, principal business activity, geographic locations, 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 operation center.
- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions.

A case study from a top financial institution demonstrates how this guidance has been put into action to create a strong TPPP management oversight program that has greatly improved the outcome of its audits, as well as provided useful information for their internal stakeholders.

Establishing a TPPP Management Program

A top financial institution with both a Merchant Acquiring and a Commercial division needed better visibility into its TPPPs and its TPPPs' customer relationships to improve its regulatory compliance. The bank used best practices from its Merchant Acquiring oversight group to establish a strong TPPP management program, using the following steps:

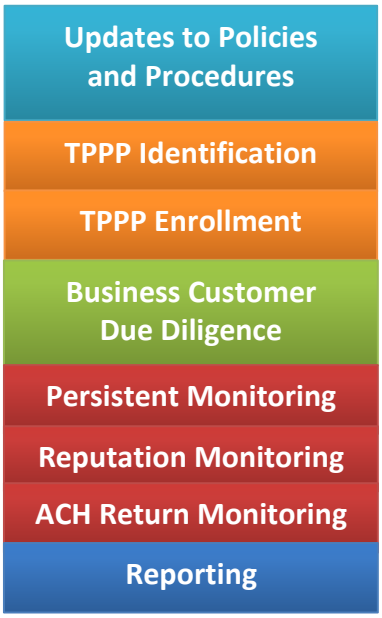
1. **Updates to Policies and Procedures:** As part of this new program, all TPPPs are required to sign new agreements stipulating they will provide information on their underlying business customers to the FI, so that these customers could be evaluated for any risk factors. This allows the FI to assess each TPPP thoroughly and decide whether or not the TPPP matched its risk appetite. Some financial institutions also publish a list of prohibited high-risk business categories to their TPPPs to ensure that its TPPP relationships align to its desired risk profile.

2. **TPPP Identification:** The new TPPP oversight group utilizes numerous functions across the company to assist in identifying its TPPP customers. This includes the Relationship Management team, Business Line Risk Managers, ACH Operations, AML Operations and Compliance.

3. **TPPP Enrollment:** All TPPPs that fit the bank's risk profile are then enrolled into the new program using new agreements that reflect the updated policies and procedures.

4. **Business Customer Due Diligence:** The bank uses onboarding solutions from G2 Web Services in its Merchant Acquiring business that it realized could also be used for its Commercial business. G2 KYC Investigate allows the bank to generate instant risk scores for its TPPPs and its TPPPs' customers at onboarding with the G2 Compass Score®, as well as detailed reports with G2 Global Boarding to understand the specific factors driving the risk score so it can make better decisions about who it wants to do business with. Based on years of proprietary data including business customer connections to undisclosed websites, links to criminal rings, fraud violations and more, G2's Solutions for Commercial Banks go beyond identity verification to provide a more comprehensive view of a business customer's risk profile.

Elements of an effective TPPP Management System



5. **Persistent Monitoring:** The bank knows from its experiences in the Merchant Acquiring division that monitoring its customers after onboarding is critical, as businesses can change over time and it is hard for banks to detect these changes. Examples of this include changes in business policies, website content, high risk business categories and more. These changes cannot be detected through transaction monitoring but can be very damaging to a bank's portfolio. The financial institution uses G2 KYC Protect — including G2 Persistent Merchant Monitoring — to understand if a particular TPPP or business customer remains suitable for them to do business with.

6. **Reputation Monitoring:** As mentioned earlier, declining reputation and complaints are leading indicators of risk that can harm a financial institution's portfolio. Reputation monitoring in the form of negative news searches and UDAAP violations is included in the TPPP oversight program to augment the FI's portfolio risk analysis.

7. **ACH Return Monitoring:** ACH return rates are also leading indicators of risk, signaling possible credit risk to the financial institution. The bank monitors ACH return rates as part of its TPPP management program to ensure that these rates stay within NACHA guidelines.

8. **Reporting:** Using the due diligence and monitoring tools mentioned above, the financial institution delivers thorough reports to all company stakeholders on a quarterly basis, including Risk Management, Compliance and Relationship Managers (RMs). It also holds regular meetings to discuss program updates and outcomes. RMs are particularly interested in the information and insights uncovered through the program about their customers. Not only does the reporting

improve its internal communications, but it has been well received during internal audits and regulator examinations.

This example demonstrates the power of combining the right tools and processes to deliver strong outcomes. In creating this program, the financial institution realized that to truly satisfy its regulatory requirements, it was important to partner with their TPPPs as opposed to just treating them as organizations to examine. By demonstrating the importance of KYC and KYCC to their TPPP customers — and by providing a solid engagement framework — the financial institution improved the outcome for all parties.

G2 Solutions for Commercial Banks

A core component of the financial institution's TPPP management program is **G2's Solutions for Commercial Banks** which combine proprietary data, advanced software and the knowledge of expert analysts to provide onboarding and ongoing monitoring solutions. These solutions help financial institutions reduce risk, improve regulatory compliance, increase operational efficiency and gain transparency into TPPP relationships, allowing them to grow their business customer portfolios.

G2 KYC Investigate helps banks learn about the risk profile of their business customers based on a combination of proprietary and third party information, including:

- Reputation history: ability to check multiple reputation databases for signs of poor reputation, a leading indicator of risk
- Fraud history: flag businesses that have past incidents of fraud to avoid onboarding them
- Watch list checks: whether anyone associated with the business appears on the OFAC, PEP, or a dozen additional watch lists
- Number of financial institution relationships: whether a business has a high number of relationships with FIs, which could signal risky behavior including money laundering

G2 KYC Investigate analyzes business customers against the G2 Business Data Map™, the most extensive database of business customer risk and fraud history available — to uncover hidden risk factors not available anywhere else. The G2 Business Data Map is comprised of over 11 years of proprietary data gathered from monitoring millions of businesses and linking billions of data points on business risk and fraud history. From the G2 Business Data Map, G2 Web Services delivers a comprehensive risk assessment using the G2 Compass Score®, an instant risk scoring solution that predicts the likelihood of fraud or compliance violations with 99% accuracy, enabling a true risk-based underwriting approach.

G2 KYC Protect provides ongoing business and content monitoring of business customer portfolios — ranging from hundreds of customers to hundreds of thousands of customers — gaining financial institutions faster updates regarding potentially harmful changes across multiple dimensions as mentioned above.

G2 KYC Protect goes beyond existing transaction monitoring services to help FIs identify risky business customer behavior before it reaches the transaction level. With KYC Protect, FIs can proactively identify high-risk business customers and closely monitor their activities, to more effectively manage both

positive and negative risk. G2 Web Services can work with you to develop and implement a program that best matches the needs of your financial institution.

Industry Resources

National Automating Clearing House Association (NACHA)
The NACHA organization plays a key role in the payments ecosystem, both as a trade organization and as the administrator of the ACH network which represents over 20% of all electronic payments made in the US. Representing over 10,000 financial institutions through 13 Regional Payments Associations (RPAs) as well as through direct membership, NACHA sets the operating rules for the ACH network, balances risk and innovation of the ACH network and provides educational resources and networking opportunities for industry professionals. Learn more at www.nacha.org.

Regional Payments Associations (RPAs)
Through RPAs, financial industry professionals can receive guidance on NACHA operating rules, as well provide feedback to help shape the rules that govern the ACH network. They can also access valuable training and other resources to stay current with industry developments. Learn more at https://www.nacha.org/members/regional-payments-associations.

Third Party Payment Processor Association (TPPPA)
The TPPPA is a non-profit industry association representing the interests of Third-Party Payment Processors and Third-Party Senders, as well as its financial institutions and its business customers. Through this organization, banks and TPPPs can align on core processes for the benefit of their respective businesses, as well as for the entire commerce industry. Learn more at www.tpppa.org.

About G2 Web Services

G2 Web Services is a leading global provider of risk management solutions, including due diligence, compliance and fraud protection. G2 helps acquirers, commercial banks and other payment providers take on the appropriate level of risk in their portfolios, while protecting against brand damage, illegal activity and noncompliance assessments. To learn more about how G2's Solutions for Commercial Banks can help your business, please contact Jackie Ostler Burke at 1-858-775-6697 or jburke@g2llc.com.

Sources

1. http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20–%2006-12-2015.pdf
2. FFIEC BSA/AML exam manual pages 136-137
3. http://files.consumerfinance.gov/f/201408_cfpb_consent-order_global-client-solutions.pdf
4. http://guardianananalytics.com/videos/samedayrisks-september2015.php
5. http://www.americanbanker.com/bankthink/fdic-responds-banks-must-manage-client-risk-on-case-by-case-basis-1073979-1.html
6. American Banker webinar “Managing AML/KYC Compliance Risk, Rather than Avoiding It”, http://pages.marketing.americanbanker.com/20150511_abp_pso_jumio_ws_lp.html