THIRD PARTY PAYMENT PROVIDERS

BY DARLIA FOGARTY, DIRECTOR OF COMPLIANCE & COO
Third Party Payment Processors (TPPPs or processor(s)) originate transactions for consumers or businesses that are not direct customers of the originating financial institution.

- They provide payment processing services to merchant or business clients, and group these payments together to take advantage of economies of scale.
- Third Party Payment Processors are one type of Third Party Service Providers (TPSP), which is a broader category of third party relationships.
Third Party Payment Processors use their deposit account at your bank to conduct payment processing on behalf of THEIR different clients.

These account remain attractive to bankers, despite the amount of risk, because they can earn an attractive amount of fee income for facilitating these transactions.
POTENTIAL RISK

- **Liquidity risk**: Processors may require the transmission of a large dollar volume from their deposit account. The Bank must monitor the average volume and remain prepared to deal with large outflows or inflows of cash.

- **Fraud risk**: Instances of merchant fraud are being detected through banks’ relationships with processors. Fraud can take many forms, from unauthorized transactions using stolen account numbers to repeated debit entries by an illegal merchant. Additionally, “the risk of fraud arises when an illicit telemarketer or online merchant obtains the consumer’s account information through coercion or deception and initiates an ACH debit transfer that may not be fully understood or authorized by the customer (FDIC).”
POTENTIAL RISK S

- **Compliance Risk**: Compliance risk can pop up from Regulation E, Regulation J, Regulation CC, BSA/AML/OFAC regulations, and ACH rules just to name a few.

- **Consumer Protection and Liability Risk**: High-risk or illegal merchants may attempt to process transactions through a processor. These transactions may be considered unfair or deceptive, as defined by the Federal Trade Commission Act. As previously mentioned, “Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor’s or merchant client’s fraudulent or unlawful activity and, thus, be liable for such acts or practices (FDIC).” In other words, if processing an illegal transaction results in harm to a consumer, the institution may be required to pay restitution and/or civil money penalties.

- **Reputation Risk**: In some cases, processors target small, community institutions because of their perceived lack of control and ongoing monitoring. In these cases, the reputational risks are heightened. For example, news of a large loss sustained from a failed processor relationship may impact the community’s perception of the safety and soundness of an institution. Also the consumer protection risk described above can result in damage to the bank’s reputation.

- **Credit Risk**: Processors’ deposit accounts can become overdrawn quickly, often due to returns and chargebacks. A troubled processor’s debt may become uncollectible, presenting credit risk to the institution.
Most payment processors effect legitimate payment transactions for a variety of reputable merchants.

However, an increasing number of processors have been initiating payments for abusive telemarketers, deceptive online merchants, and organizations that engage in high risk or illegal activities.

The Bank must have adequate due diligence processes and other controls in place to protect themselves.
Managing Third Party Payment Processor risk is the same as managing any other risk in the bank. The Bank must create a robust program that includes:

- Risk Assessment
- Policies
- Procedures
- Due Diligence
- Oversight
Managing risk presented by TPPPs may be harder than you can imagine.

The Bank does not have a relationship with the processor’s merchant clients – that is the tricky part.

The Bank must ensure that the TPPP that they are doing business with is conducting adequate due diligence on their merchant clients including:

- Verifying identities and business practices
- Implementing a program of ongoing monitoring for suspicious activity
Third Party Payment Processors most frequently offer their clients payment services via the ACH network or remotely created checks (demand drafts).

The FDIC has observed that some of the most problematic activity occurs in the origination of ACH debits or the creation and deposit of remotely created checks.
The TPPs initiate ACH debit transfers as payments for merchant clients by submitting transfers, which contain the consumer’s routing number and account number.

The TPPPs gets the account information from their merchant client to initiate the ACH debit transfer.

Fraud can occur when an illicit telemarketer or online merchant obtains the account information through coercion or deception and initiates the ACH debit transfer that may not be fully understood or authorized by the consumer.
The Bank bears the responsibility of implementing an effective system of internal controls and ongoing account monitoring for detection and resolution of fraudulent transfers.

Under Regulation E, the consumer has 60 days after the Bank sends an account statement to report the unauthorized ACH debit.

In the case of ACH debits, the ACH rules permit the consumer’s bank to recover the amount of the unauthorized payment by returning the debit item to the originating financial institution – which means YOU pay.
These are payment instruments that do not bear the signature of a person on whose account the payments are drawn. Instead, it has the account holder’s printed name and a statement that the account holder has authorized the issuance of the check.

This is another method of payments provided to TPPP’s merchants.

The risk of fraud here is great!

The Bank must implement an effective system of internal controls and account monitoring to identify and resolve unauthorized RCCs.
- Can be processed as paper item – governed by UCC
- Can be processed as an ACH debit – governed by ACH rules and Regulation E
- Amendments to Regulation CC and Regulation J shifted the liability for losses attributed to unauthorized RCCs to the financial institution where the check is first deposited as this institution is in the best position to know its customer (the creator of the RCC) and determine the legitimacy of the deposits.
- This also creates a greater incentive for banks to perform enhanced due diligence on their customers depositing RCCs.
- This also made it easier for customers to obtain re-credits for unauthorized RCCs.
The bank should identify “high risk” processors.

These are processors who are disreputable as they may charge for questionable or fraudulent goods, charge a higher fee than advertised, or enroll customers in costly plans without their full understanding and consent.

Also included may be processors who initiate payments for unlawful internet gambling or the illegal sale of tobacco products on the internet.

Generally, high-risk transactions occur when the consumer does not have a familiarity with the merchant, or when the quality of the goods and services being sold is uncertain.

Activities involving purchases made over the telephone or on the Internet tend to be riskier in that the consumer cannot fully examine or evaluate the product or service purchased. Similarly, the consumer may not be able to verify the identity or legitimacy of the person or organization making the sale.
Complaints – more on the next slide.

Large number of returns or charge backs - must monitor for this.

Significant amount of activity which generates higher than normal level of fee income – fee income is needed in banks. However, a higher level of fee income from TPPPs indicates an increased level of risk.

The use of more than one bank to process merchant client payments - Spreading the activity among several institutions may allow processors that engage in inappropriate activity to avoid detection.

Processors that purposefully solicit business relationships with struggling banks that need the fee income - Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.
One of the more telling signs is a high volume of consumer complaints that suggest a merchant client is:

- inappropriately obtaining personal account information;
- misleading customers as to the quality, effectiveness, and usefulness of the goods or services being offered; or
- misstating the sales price or charging additional and sometimes recurring fees that are not accurately disclosed or properly authorized during the sales transaction.

May prove to be difficult since the bank may not be privy to complaints submitted directly to the processor.

Check the Better Business Bureaus and other websites/blogs where customers often go to complain or share unfavorable information on businesses.
The bank must understand that some complaints may name the Bank since the bank’s name will appear on the face of the RCC or in the record of an ACH debit.

Consumer may associate the bank with the unauthorized transaction.

The bank must acknowledge, research and respond to each complaint made directly to them.
RISK CONTROLS

- Establish clear lines of responsibility for controlling the associated risks
- Effective due diligence and underwriting
- Ongoing monitoring of high risk accounts for an increase in unauthorized returns, charge backs, suspicious activity and/or complaints
- Maintenance of adequate balances or reserves to cover expected high levels of returned items
- Ensure the relationship is governed by a written agreement/contract
- Implement appropriate controls over processors and their merchant clients to identify processors working with fraudulent or unscrupulous merchants to avoid such transactions
Appropriate oversight and monitoring of these accounts may require the involvement of multiple departments, including information technology, operations, BSA/anti-money laundering (AML), and compliance.
DUE DILIGENCE AND UNDERWRITING

- Implement policies and procedures that reduce the likelihood of establishing and maintaining a relationship with payment processors through which unscrupulous merchants can access customers’ deposit accounts.

- Implement a processor approval program that extends beyond credit risk management, including:
  - Background checks of payment processors and merchant clients
  - Validate activities, creditworthiness, and business practices of payment processor
  - Authenticate the processor’s business operations
  - Assess their risk level
Identifying the major lines of business and volume for the processor's customers;

Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants;

Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners;

Reviewing the processor's promotional materials, including its Web site, to determine the target clientele;
Determining if the processor re-sells its services to a third party that may be referred to as an agent or provider of "Independent Sales Organization opportunities" or a "gateway arrangement" and whether due diligence procedures applied to those entities are sufficient;

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; and,

Determining whether any conflicts of interest exist between management and insiders of the financial institution.
The Bank should require information on the TPPPs’ merchant clients such as name, principal business activity, geographic location, and sales techniques.

The Bank should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business.

Such verification could include comparing the identifying information with public record, fraud databases and a trusted third party, such as a credit report from a consumer reporting agency or the state Better Business Bureau, or checking references from other financial institutions.

The same information should be obtained if the merchant uses sub-merchants (or affiliates).
Implement systems that monitor for higher rates of returns or charge backs and/or high levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds, all of which often indicate fraudulent activity. This would include analyzing and monitoring the adequacy of any reserve balances or accounts established to continually cover charge-back activity.

The bank is required to have a Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program and appropriate policies, procedures, and processes in place for monitoring, detecting, and reporting suspicious activity – this program should be used to conduct ongoing monitoring.

TPPPs are mostly non-bank processors that are generally not subject to BSA/AML and thus more susceptible to money laundering, identity theft, fraud schemes, and illicit transactions.

The Bank’s monitoring program must include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.
- Establish procedures for regularly surveying the sources of consumer complaints that may be lodged with the payment processor, its merchant clients or their affiliates, or on publicly available complaint Web sites and/or blogs. This will help the institutions identify processors and merchants that may pose greater risk.

- The bank should have a formalized process for periodically auditing 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.
Formal actions have included Cease and Desist Orders under Section 8(b) or 8(c) of the Federal Deposit Insurance (FDI) Act, as well as assessment of Civil Money Penalties under Section 8(i) of the FDI Act.

These orders have required the financial institution to immediately terminate the high-risk relationship and establish reserves or funds on deposit to cover anticipated charge backs.
The examiner will determine if financial institution management has knowledge that the payment processor or the merchant clients are engaging in unfair or deceptive practices in violation of Section 5 of the Federal Trade Commission Act.

In those cases where a financial institution does not conduct due diligence, accepts a heightened level of risk, and allows transactions for high-risk merchants to pass through it, it may be determined that the financial institution is aiding and abetting the merchants.

This also could indicate a disregard for the potential for financial harm to consumers and, as a result, the financial institution may be subject to civil money penalties or required to provide restitution.
Thank you for your participation!
We hope you found value in today’s presentation.

If you have any additional questions,
contact Compliance Alliance at 888-353-3933.