Regulatory Compliance

Understanding the laws and regulations that apply to you if you take payments

One aspect of risk that a company faces when processing payments is the possibility of laundering illicit funds or financing terrorist activity. For those new to the payments industry, the regulations that aim to mitigate these activities can be complex and difficult to understand. This document will lay out the basics of financial regulatory compliance around money laundering and terrorist financing and how WePay manages this risk on behalf of our partners.

Anti-Money Laundering (AML)

The government requires financial institutions and payment processors to actively avoid knowingly laundering money, and therefore, are required to implement controls to detect and deter this activity.

Here is one of the simplest examples of money laundering on an online platform. A drug dealer has ten thousand dollars in dirty cash. They go to a big retailer, purchase and load their cash onto gift cards, and process them all as donations to a crowdfunding campaign they set up using one of WePay's platform partners. Then they withdraw the money to a bank account. The reason for this is twofold. Banks are required to report large deposits of cash to the government and typically will ask where the cash came from. In addition, moving the money around makes it harder to trace the source of the funds.

WePay's AML program is designed with both automatic and manual processes to detect this and other types of suspicious activity and prevent them. We have a wide range of rules and reports that we use to screen all transaction activity, and a dedicated risk and compliance operations team that reviews and actions accounts every day.

So what do you need to know about AML? Regulators direct financial institutions to develop a program to mitigate and address this risk and to do so at a level that is proportionate to the risk of the particular circumstances of your service. Failing to appropriately mitigate the risk of money laundering can lead to huge fines. For example, Deutsche Bank was fined $630 million in 2017 for failing to prevent money laundering.

Economic Sanctions and Terrorist Financing

Another significant risk that companies face is facilitation of terrorist financing and other transactions against U.S. economic policy. Not only can failures in this area lead to grave public and social consequences, but can also be reputationally catastrophic for all institutions involved. Fines and penalties in this area, just like with money laundering, can be significant. In 2012, HSBC paid over $1.2 billion for a range of infractions.

In order to mitigate this risk, WePay screens every name that passes through our systems against names associated with terrorism and terrorist financing. These lists come from the U.S. government and global entities associated with tracking terrorism. We continue to refine our monitoring tools to be able to catch the bad guys while also minimizing false positives, which are individuals and entities whose characteristics trigger a screening match to entries on these government lists, but who, after a review, are determined not to be true hits.

Though WePay assumes regulatory compliance risk for our partners, your organization should strive to be aware of the regulations in this area and, more importantly, the potential risk your customers may pose in this regard. We ask that our partners be prepared to proactively follow up with customers and with WePay in the instances that your or WePay identifies suspicious activity.

For more information on the challenges of payment regulation see: https://www.wepay.com/api/payments-101/payment-regulation-challenge or contact sales@wepay.com.