POLICY ALERT // MAY 29, 2019

OFAC Kingpin Sanctions Highlight Payment Processor Risk

The Treasury Department's Office of Foreign Assets Control (OFAC) on May 23, 2019 sanctioned a network running online pharmacies and an associated payment processor, providing a revealing glimpse into how criminal organizations are exploiting retail payment networks to engage in illicit conduct. Despite a proliferation of new payment methods during the past 10 years, card-based payments continue to account for more than half of all consumer payments, and cards' share of payments is expected to grow through at least 2022.[1] Credit and debit card acceptance can be critical enablers for criminal organizations seeking to sell illicit goods to U.S. consumers directly, because consumers expect merchants to accept cards, especially for online transactions, judging from press reporting on consumer spending habits.[2]

- OFAC on May 23, 2019, sanctioned eight Argentine nationals for their roles in Goldpharma, a network of online pharmacies based in Buenos Aires.[3] Goldpharma sold both legitimately and clandestinely produced narcotics, including Oxycodone, Hyrdocodone, and Tramadol, to customers without prescriptions.[4] Most of Goldpharma's customers were in the United States.[5]

- OFAC that same day sanctioned three Argentine nationals for their roles in a multi-country network of companies known as the Smile Group, which funnels drug proceeds back to Goldpharma.[6] The Smile Group's U.S. presence includes three Texas companies, two Delaware companies, and two Florida companies, all of which were also sanctioned by OFAC.[7]

- One of the Smile Group's entities, Smile Payments, offers international credit card payments, point-of-sale terminals, prepaid cards, and Bitcoin trading, and claims to have relationships with major credit card system operators and online payment systems.[8] The company courts customers engaged in high-risk businesses such as adult content, online gaming, health and wellness products, dating, and call centers.[9]

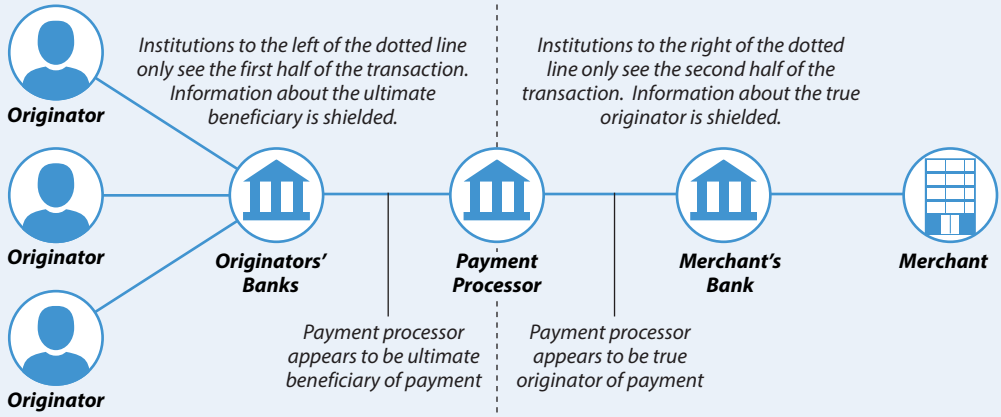
Payment processors face lower regulatory barriers to entry in many countries than banks or money services businesses, making them attractive vehicles for money launderers. In the United States, payment processors intermediating payments solely between financial institutions regulated under the Bank Secrecy Act (BSA) are exempt from money transmission transparency requirements.[10]

- Payment processors lengthen payment chains and can be used to obscure

the financial relationship between the originator of a payment and the beneficiary of the payment, particularly when the payment is being effected through a channel that is exempt from the travel rule, such as an automated clearinghouse or point-of-sale-system.[11]

- As of 2018, several countries had reported the use of payment processors by suspected money laundering networks, according to the Financial Action Task Force (FATF).[12]
- Payment processors have been used to launder money for mail fraud schemes[13] and illicit online gambling.[14] In some mail fraud schemes, a payment processor was used to "minimize the chance that financial institutions will detect the scammers and determine their activity to be suspicious," according to OFAC.[15]

How Payment Processors Can be Exploited to Conceal Information



As payment processors have evolved and caused payment chains to be extended or further intermediated, they have made risk management more difficult throughout the financial system because they can be used as middlemen to obscure the source, destination, or purpose of a funds transfer. Payment processors are not merely invisible intermediaries in payment chains. Some payment processors repackage or aggregate payments in a manner that reduces visibility into the payments for the banks involved, which reduces the value of funds transfer information in identifying the underlying economic activity associated with a payment or in discovering links between bank customers and sanctioned or other illicit actors.

- In February 2019, the California Department of Business Oversight noted that payment chains were becoming "longer and more convoluted" and sought comments on whether and how to clarify its money transmission regulations.[16]
- As of March 2019, Danish authorities were contemplating additional regulation on companies that provide payment services because they were concerned that payments were becoming more complex.[17]
- The head of risk management at a European bank complained in March 2019 that she was concerned that her bank would not have enough information to block payments that were prohibited by sanctions when those payments were routed through payment processors.[18]

Banks are vital gatekeepers to retail payment systems and should recognize that payment processors, including fintech companies involved in payments, present intermediated risk and that banks have reduced visibility into customer activity when those customers are heavy users of payment processors. *(See Payment Processor Red Flags, following page)* In addition to money laundering and sanctions evasion, payment processors can also be exploited by companies seeking to evade the value added tax (VAT) in jurisdictions that have implemented a VAT.[19]

- For payment processor customers, banks should implement procedures similar to those procedures used for correspondents. In particular, banks should understand the beneficial ownership of the payment processor and the risk profile of the payment processor's customers. After onboarding a payment processor, banks should monitor the payment processors' accounts closely to ensure that their actual activity is closely aligned with their expected activity.
- Banks' extensive due diligence should include a review of payment processors' sanctions compliance programs and their anti-money laundering (AML) programs. Although exempt from money transmission rules under the BSA in the United States, many payment processors have established AML programs voluntarily.
- For retail or corporate customers that conduct a large proportion of their transactions through payment processors, transaction monitoring will be less effective in detecting unusual activity because less information will be available about the customer's payments than is available for other customers. Banks should conduct enhanced due diligence on customers that conduct a large proportion of their transactions through payment processors, both at onboarding and during periodic refresh.

Payment Processor Red Flags

In 2012, FinCEN published red flags for payment processor relationships that were developed by the Financial Fraud Task Force's Consumer Protection Working Group.[20]

- **Fraud**: High numbers of consumer complaints and high numbers of returns or chargebacks suggest that the merchant may be engaged in unfair or deceptive business practices.
- **Accounts at multiple financial institutions**: Payment processors engaged in suspicious activity often maintain accounts at more than one financial institution or may quickly move among financial institutions.
- **Foreign-located payment processors**: Relationships with foreign-located processors pose heightened risk.
- **Solicitation for business**: Payment processors engaged in suspicious activity have solicited business relationships with distressed financial institutions in need of revenue and capital.
- **High rates of return for debit transactions**: Payment processors engaged in suspicious activities may have substantially higher average rates of return for debit items due to unauthorized transactions.

FIN assesses that additional red flags may be useful in helping financial institutions detect illicit payment processors, based on an analysis of payment processors' offerings.

- **Customers in high-risk industries**: A large share of the payment processor's customers are in high-risk industries or the payment processor openly solicits customers in high-risk industries, making the payment processor higher risk for illicit finance.
- **High fees**: The payment processor charges fees that are much higher than the industry average, suggesting that it may be engaging in money laundering.
- **Terms of service**: The payment processor does not make its terms of service available on its website, or its terms of service fail to include industry standard provisions such as a selection of venue and choice of law for resolving disputes.

Endnotes

1 Wall Street Journal, "Meet the New Payment Champions, Same as the Old Ones," Jan. 11, 2019, https://www.wsj.com/articles/meet-the-new-payment-champions-same-as-the-old-ones-11547202620.

2 Wall Street Journal, "Meet the New Payment Champions, Same as the Old Ones," Jan. 11, 2019, https://www.wsj.com/articles/meet-the-new-payment-champions-same-as-the-old-ones-11547202620.

3 Treasury Department, "Treasury Sanctions Argentina-based Goldpharma," May 23, 2019, https://home.treasury.gov/news/press-releases/sm694.

4 Treasury Department, "Treasury Sanctions Argentina-based Goldpharma," May 23, 2019, https://home.treasury.gov/news/press-releases/sm694.

5 Treasury Department, "Treasury Sanctions Argentina-based Goldpharma," May 23, 2019, https://home.treasury.gov/news/press-releases/sm694.

6 Treasury Department, "Treasury Sanctions Argentina-based Goldpharma," May 23, 2019, https://home.treasury.gov/news/press-releases/sm694.

7 Treasury Department, "Treasury Sanctions Argentina-based Goldpharma," May 23, 2019, https://home.treasury.gov/news/press-releases/sm694.

8 Smile Payments, "Partner Program," undated, http://smilepayments.com/en/partner-program/.

9 Smile Payments, "Rates," undated, http://smilepayments.com/en/rates/.

10 See 31 CFR 1010.100(ff)(5).

11 See 31 CFR 1010.100(w)(5).

12 Financial Action Task Force, "Professional Money Laundering," July 2018, http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf.

13 Treasury Department, "Treasury Sanctions Individuals and Entities as Members of the Pacnet Group," Sept. 22, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl5055.aspx.

14 Justice Department, "AUSTRALIAN MAN CHARGED IN MANHATTAN FEDERAL COURT WITH LAUNDERING HALF BILLION DOLLARS IN INTERNET GAMBLING PROCEEDS," April 16, 2010.

15 Treasury Department, "Treasury Sanctions Individuals and Entities as Members of the Pacnet Group," Sept. 22, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl5055.aspx.

16 California Department of Business Oversight, "INVITATION FOR COMMENTS ON PROPOSED RULEMAKING MONEY TRANSMITTER ACT: AGENT OF PAYEE," Feb. 8, 2019, http://www.dbo.ca.gov/Licensees/money_transmitters/PRO-07-17-Agent-of-Payee-Invitation-for-Comment-FINAL.pdf.

17 Bloomberg, "After Danske, New Dirty Money Risk Seen in Payment Services," March 17, 2019, https://www.bloomberg.com/news/articles/2019-03-17/after-danske-next-dirty-money-route-gets-scrutinized-in-denmark.

18 Bloomberg, "After Danske, New Dirty Money Risk Seen in Payment Services," March 17, 2019, https://www.bloomberg.com/news/articles/2019-03-17/after-danske-next-dirty-money-route-gets-scrutinized-in-denmark.

19 Her Majesty's Treasury, "Tackling tax avoidance, evasion and non-compliance," November 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661531/tackling_tax_avoidance_evasion_and_non-compliance.pdf.

20 FinCEN, "Risk Associated with Third-Party Payment Processors," Oct. 22, 2012, https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A010.pdf.