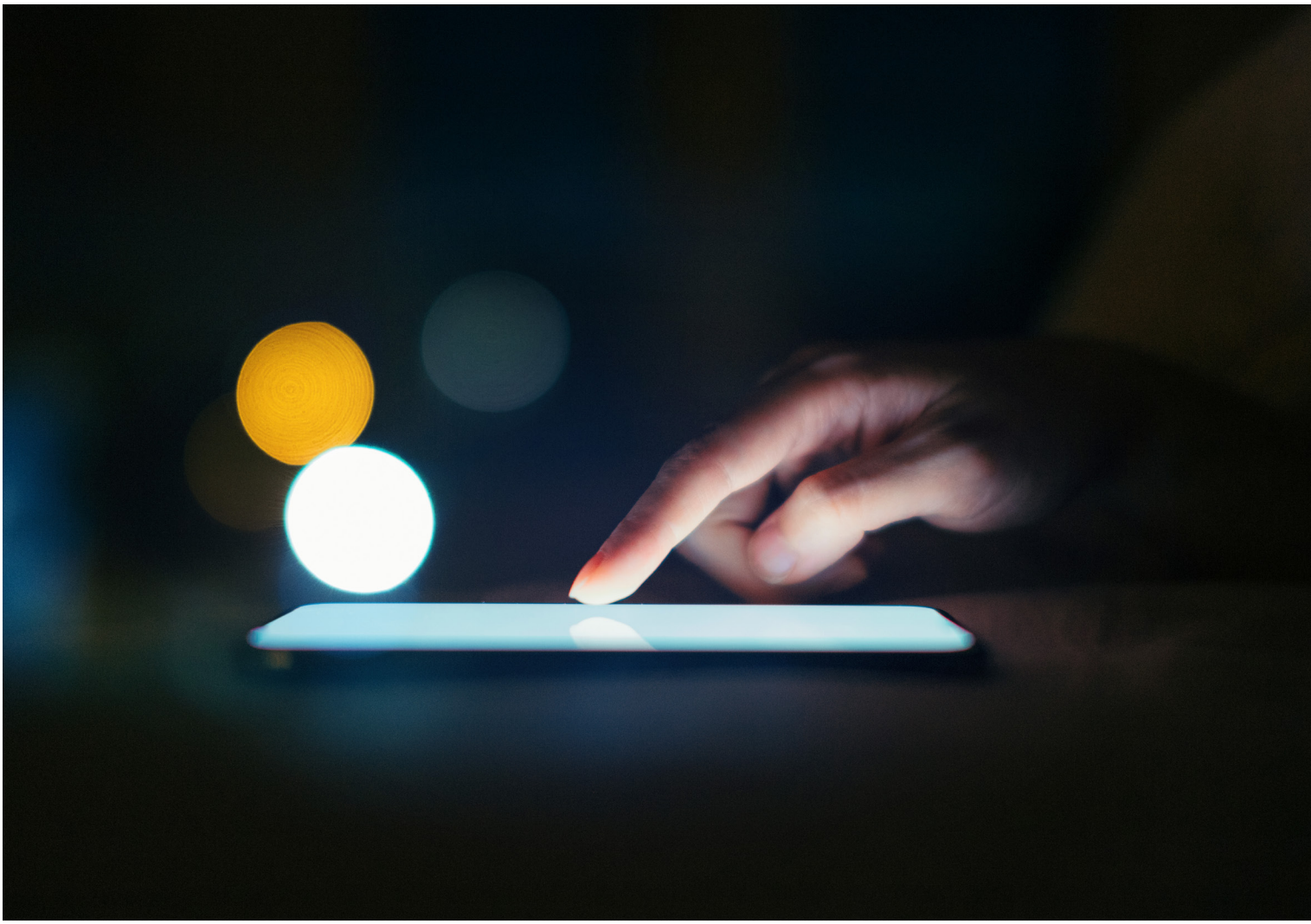
protiviti®

Face the Future with Confidence



Clean Money Is a Click Away

The Money Laundering Risks of E-Commerce

Internal Audit, Risk, Business & Technology Consulting

The global e-commerce market is projected to approach $5 trillion in sales in 2021[1] — pretty impressive for an industry that only came into existence in 1991 when the internet was opened for commercial use. With brick-and-mortar stores shuttered because of COVID-19 and online buying the only option many consumers had, retail e-commerce sales in 2020 grew by double-digits in every region of the globe, ranging from 15.5% in Asia Pacific to 21.5% in Central and Eastern Europe.[2]

Although growth rates are expected to moderate with the re-opening of traditional retailers, the compound annual growth rate for e-commerce globally for 2020 – 2024 is forecast at 8.1%[3] That's good for online merchants and platforms. It's good for money launderers, too. After all, why would a money launderer hassle with the physical transport of ill-gotten gains or risk dealing with financial institutions with savvy detection capabilities when laundering money can be done with a few clicks of a computer in an environment that may not always be vigilant in detecting fraud?

It's obvious alleged criminals have already identified the potential for laundering funds through e-commerce. Headlines such as the following make this clear:

- Police Allege Money Launderers Using Chinese E-Commerce Sites to Move Money
- Kuwaiti Ecommerce Platform Boutiqaat Being Investigated for Money Laundering
- 313 People Arrested for E-Commerce Scams and Money Laundering Totaling Over $1.2 Million
- FBI Reveals ISIS Uses Transaction Laundering

However, money laundering was happening in the retail sales industry long before the proliferation of e-commerce. Large sums of cash used to buy high-end goods, overpayment of retail credit cards that result in a refund check appearing to be clean money, and identity theft are among the common methods of traditional retail sales money laundering. These methods are still available to money launderers, but likely less attractive when e-commerce offers the opportunity to move more money faster.

E-commerce money laundering or transaction laundering is the process of leveraging e-commerce and merchant processing to create fictitious transactions that appear legitimate.[4] These transactions may involve knowing or unknowing participants in the e-commerce ecosystem, a network of interconnected parties involved in the buying and selling of goods and services.

[1] Ethan Cramer-Flood, Global Ecommerce Update 2021: Worldwide Ecommerce Will Approach $5Trillion This Year, eMarketer, January 13, 2021: www.emarketer.com/content/global-ecommerce-update-2021

[2] The Future of Ecommerce Report 2021: Shopify Plus' Annual Report on Global Commerce Trends, Shopify Plus: **https://bit.ly/2X9buZF**

[3] The Future of Ecommerce Report 2021.

[4] Michael Schidlow, "Ghost Laundering (Part 1): Transaction Laundering's Online Twin Grows in Popularity," Thomson Reuters, September 25, 2018: www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/ghost-laundering.

Transactions may be facilitated by front companies that appear to sell legitimate goods and services but are set up by money launderers to provide cover for their illegitimate activities, pass-thru companies set up by third parties and used by one or more criminals, or funnel accounts in which payment processors may commingle legitimate and illegitimate transactions. They may involve the sale of fake or contraband goods, the value of e-commerce transactions may be over-inflated, or the transactions may simply be nonexistent, a scheme sometimes referred to as ghost laundering.[5]

Think of transaction laundering as an updated version of trade-based money laundering. Transaction laundering is difficult to detect for a number of reasons including the complexity of the payments network, the growth in alternative payment methods, the inability of merchants to safeguard their websites from being used illegally, and the use of hidden websites.

Here's a simple example of how transaction laundering could work:[6]

- John, a drug dealer, sets up a site on an e-commerce platform that facilitates peer-to-peer (P2P) sales.
- John lists a particular item for sale, and he sends the link for the item to one of his drug buyers. The value of the item appears a little high, but not so much that it raises undue concerns with the e-commerce platform provider.
- John's drug buyer "purchases" the item by sending funds through an online payment platform, crediting the funds to John's bank account.
- Both the e-commerce platform and the online payment platform receive a fee for the transaction.
- To legitimize the transaction, John may even send a box of rocks or even an empty box to his drug customer, or maybe doesn't bother sending anything at all, assuming no one is actually monitoring the movement of items sold.
- Once the payment is received, John meets his buyer to hand over the drugs.
- The transaction appears legitimate to John's bank and doesn't raise the sorts of questions John might receive from his bank if his drug deals involved depositing large volumes of cash.
- John has successfully laundered the proceeds of his drug sale — and moves on to the next deal.

Now, imagine that John is not a lone drug dealer, but the leader of a crime syndicate that sells drugs or illegal arms or runs an illegal online gambling operation or a human trafficking ring — a syndicate with vast earnings power and a newfound way to obtain and move illicitly gained funds by exploiting e-commerce and payment-platform vulnerabilities. John doesn't engage in one-off sales to his customers; he sets up a complex maze of legitimate and fake websites to conduct a large-scale, global operation. Think of the potential.

[5] "Ghost Laundering (Part 1)."

[6] PYMNTS.com, "How The eCommerce Fakers Launder Money," August 3, 2018: https://www.pymnts.com/news/security-and-risk/2018/trulioo-ecommerce-onboarding-fake-merchants-money-laundering/

Trade-based money laundering has been around for a long time and is a very common method of money laundering. So, why did it take so long to recognize that an updated version of trade-based money laundering was occurring in e-commerce?

There are a number of reasons that would explain this. First, global money laundering efforts have historically and understandably been focused on laundering in the $400 trillion-plus financial services sector, where money laundering risks have been long recognized.[8] Second, the e-commerce market, as noted above, has grown very quickly and is highly dispersed with more than 24 million e-commerce sites on the internet — and establishing an e-commerce site is decidedly easier than establishing a financial institution.

Third, there is no uniform framework for e-commerce anti-money laundering (AML) regulation and supervision. To their credit, regulators will often observe market developments for some period of time before they impose regulations that may frustrate innovation. That means that regulation often has to play catch up with reality. The AML regulatory framework for e-commerce providers is disparate, more so than that of the financial services industry, which despite national nuances, is grounded in the Forty Recommendations of the Financial Action Task Force (FATF). In some jurisdictions, e-commerce activities require providers to register as money services businesses, which in turn does subject them to some AML requirements. In other jurisdictions, e-commerce platforms are treated as payment providers with limited, if any, scrutiny of their money laundering risks.

"All e-commerce sites and payment providers have one thing in common no matter their size: the constant and pervasive threat of money launderers using their businesses to process ill-gotten gains, conceal the funds' sources and convert them into clean, taxable income that government authorities cannot track."[7]

Fourth, as proven time and time again, the bad guys are very clever and keeping up with them is a challenge for all industry sectors. While the scale of transaction laundering is difficult to quantify, one industry observer suggested more than three years ago that the global volume of transaction laundering exceeded $350 billion.[9]

In another attempt to describe the dimension of the problem, Thomson Reuters referenced[10] the following information released by the Electronics Transactions Association (ETA):

- About 50–70% of online sales for illicit drugs, counterfeit goods and unlawful adult content involve some form of transaction laundering.
- More than 90% of illegal gambling sites make use of transaction laundering to move their credit card receipts into the payment system.
- Between 35,000 and 45,000 rogue internet pharmacies are online at any one time and illicit pharmacies are only one segment of the much larger $450 billion counterfeit goods market.

[7] PYMNTS.com, "Deep Dive: How eCommerce Payment Providers Sniff Out Money Launderers," October 7, 2020: https:/www.pymnts.com/aml/2020/ecommerce-payments-aml/

[8] "Total Assets of Global Financial Institutions From 2002 to 2019," Statista, February 8. 2021: www.statista.com/statistics/421060/global-financial-institutions-assets.

[9] Elena Van de Sande, "The Digital Evolution of Money Laundering (Exclusive Interview)," goEmerchant, August 3, 2017: http://blog.goemerchant.com/digital-evolution-money-laundering.

[10] "The Growing Threat of Transaction Monitoring: What Banks and Processors Need to Know to Safeguard the Payment System — and Themselves," Thomson Reuters: https://store.legal.thomsonreuters.com/law-products/solutions/clear-investigation-software/anti-money-laundering/the-growing-threat-of-transaction-laundering.

Currently, the nature of the activities offered by the e-commerce provider is the trigger for determining how AML obligations apply, and requirements can vary significantly from jurisdiction to jurisdiction. In the United States, for example, this means that e-commerce providers generally are required to be licensed as money services businesses (MSBs). In other jurisdictions, such as the European Union and Singapore, e-commerce providers are governed as payment providers. In Hong Kong, e-commerce companies are required to file Suspicious Activity Reports but have no other explicit AML obligations.

Having a more mature AML regime will not eliminate money laundering in e-commerce. That's clear from experience with the financial services industry. What it would do, however, is heighten the e-commerce industry's sensitivity to the risks of money laundering, making it a little more difficult for criminals to exploit vulnerabilities.

Until regulation catches up with reality, online retailers and payment platform providers need to take proactive steps to prevent the e-commerce ecosystem from the risks of money laundering and terrorist financing. The principles for effective management of these risks in e-commerce parallel those that guide financial institution AML compliance:

- Appointment of a qualified AML compliance officer to direct and manage compliance efforts
- Development and adoption of policies, procedures and controls, including transaction monitoring systems, commensurate with the online retailer's or payment processor's risks.
- Employee awareness and training
- Periodic independent testing of the compliance program
- Know Your Customer (KYC) for P2P activities
- Know Your Partner (KYP) and Know Your Transaction (KYT) for business-to-business (B2B) or business-to-people (B2P) activities

KYP is the process of performing initial and ongoing due diligence of all business partners with which an e-commerce platform or payment platform is involved, including all merchants. This would include, for example, researching a merchant's business, its principals and officers; considering how long a merchant has been in business; and determining whether the merchant's website appears credible and offers products and services consistent with the merchant's description of its business, that the price of goods and services is consistent with market exp ectations, and that rep orted revenues are in line with expectations and peers. KY P, like KYC, is A ML Compliance 101 — basic, but important.

KYT goes a step further. It is the process of using transactional analysis to examine a merchant's business. By looking at transactional data (e.g., transaction velocity, frequency, time and location), real-time analysis can link the data to specific sites, link sites with other sites, and identify trends and patterns that may warrant additional investigation, such as identifying which buyers are located in high-risk jurisdictions or that transaction activity occurs in short spurts rather than occurring throughout the day. Making sense of the vast volumes of data allows e-commerce market participants to identify red flags and emerging risks before they become unmanageable problems.

Proactively addressing the risks of money laundering is the best way for e-commerce companies to forestall regulations and, just as importantly, protect their own company names from being in the headlines.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Carol Beaumier
Senior Managing Director
Asia-Pac Financial Services Practices Leader
+1.212.603.8337
carol.beaumier@protiviti.com

Carol Raimo
Managing Director
Consumer Products and Services Industry Leader
+1.212.603.8371
carol.raimo@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®