# The 2023 Threat Landscape

## A Report on Trends in Illicit Ecommerce Activity

 | 

TABLE OF CONTENTS

# The 2023 Threat Landscape: A Report on Trends in Illicit Ecommerce Activity



# Introduction

EverC is on a mission to keep ecommerce safe from illicit products and services. Our team of domain experts works to identify the patterns and practices of illicit activity in ecommerce, in a constant effort to protect our customers (and their customers) against bad actors who leverage the internet to perpetrate crimes.

To that end, we present our annual threat landscape report, which details the ongoing and trending challenges faced by those who operate in the payments ecosystem: Banks, acquirers, payment providers, and marketplaces. The data in this report has been generated from several sources, including evidence from our proprietary database, guidelines from card schemes, research from our team of industry experts, and deep investigations from our Risk Insight Services team throughout 2022.

We analyze this information to gain insights into the world of ecommerce, empowering our customers in the fight against illicit activity online.

The online world has changed, and it will continue to change. We are no longer watching out for individual hackers who hide in the deep and dark web, coming up for air and then disappearing until the next quick hit. Today's bad actors are fast, persistent, and frighteningly collaborative.

It's not just a criminal. It's a criminal network that can levy a disastrous impact on everyone in the ecommerce chain — from buyers, to sellers, to the banks and acquirers that enable payment processing, to the giant marketplace platforms where all these players join up to conduct business.

Our experts have identified several trends that capitalize on this unified threat landscape, to enable key players in the payments industry with the ability to protect against and neutralize these threats whenever possible.

# Card Scheme Expectations: Rules and Responsibilities

"An acquirer that contracts with a payment facilitator or marketplace is responsible for all acts, omissions, and other adverse conditions caused by the payment facilitator and its sponsored merchants or the marketplace and its retailers"

According to VISA

Major card brands maintain compliance guidelines to help acquirers assess and mitigate potentially illicit activity. This can include suspicious behavior, illegal acts, or simply actions that could negatively affect the card brand and other stakeholders in the payments network. These rules are designed to protect not only the card scheme, but its partnering acquirers, merchants, and cardholders.

Acquirers serve as gatekeepers designated with the task of preventing bad actors from exploiting the payments system. Within this framework, acquirers assume responsibility for associated financial entities, such as payment facilitators or marketplaces, after screening for risk exposure.

This liability includes risks associated with third-party agents and high-brand risk merchants, such as non-financial institutions dealing with cryptocurrency assets, or sellers who may later become involved in fraudulent or illicit activity.

To support risk mitigation efforts on behalf of acquirers and other financial institutions, VISA's Global Brand Protection Program (GBPP) recommends implementing robust underwriting and detection protocols as well as contracting with third parties known as Merchant Monitoring Service Providers (MMSPs). Mastercard's Business Risk Assessment and Mitigation (BRAM) outlines similar guidance.

Financial institutions are also required to conduct transaction monitoring on an ongoing basis, perform velocity checks and fraud detection mechanisms, as well as maintain sufficient reporting protocols.

Acquirers found to be processing any illicit or brand damaging transactions may therefore expose themselves and their contracting entities to compliance action, financial loss, reputational damage, or disqualification from card scheme programs. Enforcement action can be triggered by processing payments for intellectual property (IP) infringing products, pharmaceuticals without prescriptions, prohibited adult content, illegal or miscoded gambling activities, and more.

# Marketplace Risk

"Marketplace risk is not just a concern for compliance and risk departments, the fallout from suspicious or fraudulent activity affects the entire business."

Marketplace risk is not just a concern for compliance and risk departments; the fallout from suspicious or fraudulent activity can affect the entire business. For instance, when marketplaces get bad press, which can include anything from a negative review to an angry customer tweet, to an article in a major newspaper, the reputational risk can have an enormous impact that echoes across many business areas: sales, customer service, compliance, and elsewhere.

According to **PYMNTS,** 56% of buyers said they would share bad experiences with colleagues and coworkers, causing potential loss of clients and revenue in the future. Thus, the reach goes far beyond the team responsible for reacting to and shutting down a violating merchant or removing a questionable product.

In fact, online marketplaces are frequent targets for the media. Stories abound about the drawbacks of online shopping behavior, such as consumer harm from products sold on marketplace platforms or proceeds illegally routed to fund extremist groups. As the US Treasury Department highlighted in its **2022 report on Terrorist Financing Risk,** a major source of funding for domestic violent extremist groups is through the sale of merchandise.

Major online marketplaces take extensive steps to continuously remove merchandise affiliated with extremist or hate groups listed on their platforms, however, certain products can slip through. Marketplaces have been called out in the press for having things like Nazi-affiliated paraphernalia funneled through their platform. Obviously, this kind of media exposure can be detrimental to the reputation of even the largest of enterprises.

**Given that marketplaces operate in an ecosystem, all stakeholders must align when to remove an at-risk product.**

## Balancing risk and business growth: The need for security

The difficulty facing marketplaces is the ongoing conflict between maintaining comprehensive compliance rigor while balancing a positive, "frictionless" customer experience.

## “Marketplaces are forced to walk a fine line between compliance and speed.”

In the payments industry and with marketplaces specifically, the goal for business growth is to make platforms as attractive and user-friendly as possible for sellers. As a model, marketplaces retain less control over the individual sale of products — even more reason for them to practice constant vigilance of financial crime.

However, mitigating risk shouldn’t compromise the merchant user experience. In order to succeed and grow, marketplaces must be able to onboard sellers and products quickly and easily, because a difficult process could cause merchants to abandon the platform.

And this is where the tug-of-war is set in motion: Compliance teams seek to enforce very strong risk control mechanisms aimed at protecting the business. Marketplaces that aspire to onboard merchants and start selling as soon as possible will often perceive strict compliance procedures as roadblocks.

Marketplaces are therefore forced to walk a fine line between compliance and speed. If too heavy of a compliance control set is implemented during onboarding, such as requiring an inordinate amount of documentation from a seller, this can slow down or halt onboarding altogether.

That said, **frictionless onboarding does not mean that zero effort should be applied during the underwriting phase.** This rigorous approach should be applied throughout the merchant lifecycle. Inadequate reviews and unsophisticated risk controls will result in a negative user experience for the merchant.

Risk assessment cannot end at onboarding, however. Merchants change their products and business practices often, and ongoing monitoring is necessary to mitigate risk. In fact, card brands regard acquirers as the entity responsible for all illicit and potentially brand damaging behavior caused by contracted entities – and this responsibility continues throughout the partnership lifecycle.

It’s important to remember that marketplaces do not have to choose between appeasing merchants and reducing risk. With the right tools and support, it is possible to effectively balance rapid growth and adequate compliance controls to prevent financial crime from proliferating across marketplace platforms.

# Trends in monitored ecosystems

Backed by our robust data and research, we will explore notable trends in EverC monitored ecosystems, with particular focus on how bad actors abuse the payments space to earn and launder illicit proceeds. It's important to note that these criminals do not exist in a vacuum, but are connected to a global network of offenders, oftentimes responsible for countless heinous crimes all over the world.

## Intellectual Property Rights Infringement

Several copyright, patent, and trademark laws prohibit the sale or distribution of unlicensed material without authorization from the rights holder. While IP rights infringement is not new to the online space, the post-pandemic boom in ecommerce led to enormous sales in IP-infringing products and services.

> Throughout 2022, 15% of notifications flagged to EverC clients were for IP Rights Infringement.

Not only do authorities and card schemes take the initiative to combat IP infringement, but brands themselves aggressively pursue violative sellers and payment platforms facilitating the sales of these products. Taken together, this indicates a considerable litigation and regulatory risk to financial institutions and their agents.

**The IP-infringing products and services listed below are included in EverC investigations:**

## IPTV

Internet Protocol Television (IPTV) refers to the delivery of television channels through IP networks instead of more traditional means, such as cable or satellite. Although there are legitimate offerings of IPTV through established television and communications companies, most online websites advertising IPTV are not operating in a legitimate or legal manner.

To many, the use of illicit IPTV providers appears to affect only the wallets of wealthy entertainment industry and streaming services garnering billions in payments from customers and subscribers. For example, the damages to legal providers of TV content in Europe is estimated to exceed three billion Euros, according to this **report.**

In addition to the fact that the sales of illegal IPTV subscriptions compromise the livelihoods of many artists and the entertainment industry as a whole, this violative practice can promote far more serious criminal activity. Many illegitimate IPTV sellers have been tied to organized crime enterprises, ranging from fraud and money laundering networks to human trafficking and arms dealing.

With every purchase of an IPTV subscription, the reseller handles the customer facing components, as the transnational criminal organizations run the streaming infrastructure. In this sense, these illegal IPTV resellers act as money mules for organized crime networks. Given the illegal nature and unauthorized redistribution of copyrighted material, transaction laundering is common amongst illegitimate IPTV providers.

Although not necessarily illegal in and of itself, many IPTV providers may also offer adult content packages. In this context, all non-face-to-face adult transactions and services are required by major card brands to be classified as Merchant Category Code (MCC) 5967 for "Direct Marketing – Inbound Telemarketing Merchants" (VISA & Mastercard). This high-risk MCC often necessitates additional due diligence and reporting requirements to ensure that the purchase of adult content or services can be properly tracked and does not violate card brand rules.

▸ Learn more about IPTV **here.**

## Cyberlockers

Cyberlockers are online storage services mainly used to host and allow access to IP rights infringing material (movies, television shows, live sports streaming, and music) while affording both the uploader and the cyberlocker itself degrees of anonymity. To earn profits, cyberlocker operators charge fees for hosting content on their networks, sometimes adding fees for faster download speeds.

In the case of major card brands, cyberlockers have a dedicated MCC and must be classified as "High-Brand Risk Merchants". For instance, an acquirer must identify all non-face-to-face cyberlocker transactions using MCC 4816, per Mastercard rules and procedures. However, illicit cyberlockers will often register under generic merchant names to operate with relative ambiguity.

Most cyberlockers also do not accept payments directly, but rather through vast networks of subscription sites to procure funds. Therefore, the risk of transaction laundering funds to keep the cyberlocker operational is very high.

In addition to IP infringing content, cyberlockers are a hotbed for the dissemination of child sexual abuse material, non-consensual pornography, and other harmful content. Processing payments for cyberlockers entails several critical risks for acquirers and other related parties.

As criminals use increasingly sophisticated methods to keep their cyberlocker services running, it is difficult for financial institutions and payment providers to prevent being unintentionally involved in these transactions. Authorities and brand compliance programs are aware of this weak point and will issue fines to acquirers for cyberlocker activity.

▸ Learn more about cyberlockers **here.**

## Illegal Pharmaceuticals

> The illicit sale of pharmaceuticals without authorized prescriptions constituted roughly 15% of notifications issued to EverC clients in 2022.

Given that the provision of medicines to individuals without a medical prescription violates the law and poses a significant danger to public health, major card brands explicitly prohibit this type of behavior.

Buying prescription medications from rogue online pharmacies can be dangerous, because you have no way of knowing if the medication has been tested for quality and safety by an approved authority.

As per VISA compliance rules, “facilitating transactions on behalf of illegal pharmacies – in any capacity – could expose those participating to reputation/brand risk, civil litigation, criminal prosecution, and financial risk, and may contribute to the serious injury or death of an individual”.

Not only have such purchases also been linked to fund terrorist and non-state armed groups trafficking medical products, but they also open the door for counterfeit pharmaceuticals to be manufactured on a massive scale and distributed to those most vulnerable. According to a **UNODC report,** fake medicines manufactured in places like China, Belgium, France, and India kill almost 500,000 sub-Saharan Africans a year.

Of course, regulatory and protective legal instruments exist to counter the illegitimate sale of medications online. However, bad actors continue to find innovative ways to penetrate the system while hiding their illicit activity. For instance, several merchants practice “squatting”, which means using legitimate companies’ archived pages or websites as landing pages to advertise and publish their illegal products.

In many cases, processing payment for the products offered on these websites are not made through the website’s payment page, but include several steps, including verification of the buyer’s identity, sending an email or phone message with a link to the payment page, or payment via untraceable cryptocurrencies, etc.

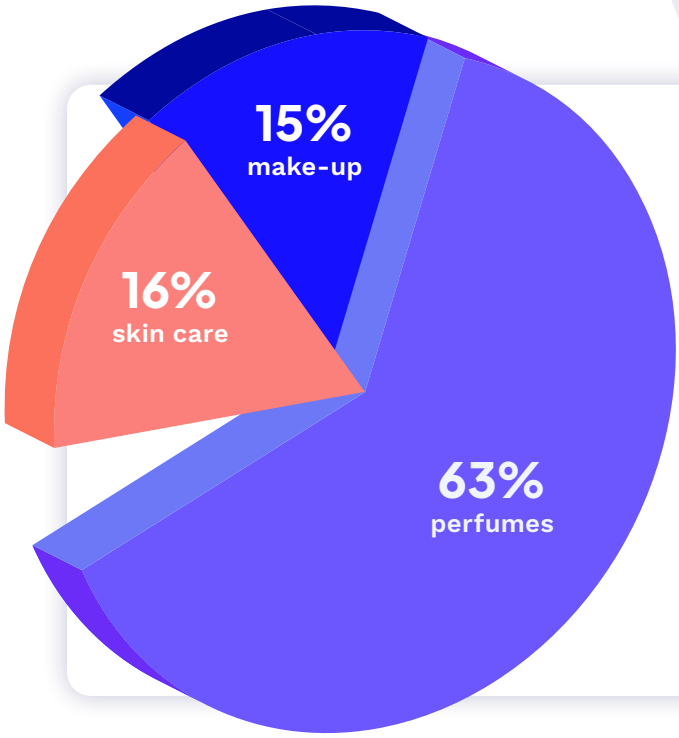
Furthermore, merchants who trade in pharmaceuticals will often delay sending the link for payment after a purchase is made on the website. This gap of time further complicates the investigative process to identify transactions related to illicit pharmaceuticals.

## Counterfeit Goods

Counterfeiting has become a huge and growing problem for online marketplaces and sometimes for payment providers as well. Spurred by the pandemic, many sellers of counterfeit goods transitioned from physical stores to ecommerce platforms, often using social media advertisements and influencers, hidden links, or drop shipping schemes to make sales.

> In 2021 alone, at least $1 trillion in pirated and counterfeit goods were sold online.

Beyond the purchase of fake luxury handbags or apparel, this also poses a serious risk to consumer health as some counterfeit goods, such as medicines, nutraceuticals or cosmetics may contain dangerous substances that cause bodily harm, lasting health effects, or even death to users. Additionally, when consumers lose faith in the authenticity of the products they purchase, the financial




In the case of fake cosmetics, **EverC solutions were able to remove over 40,000 counterfeit products** from our partnering marketplaces in 2022. This included perfumes (63%), skin care (16%), and make-up (15%), for **combined worth of more than $2 million USD** prevented from reaching the pockets of criminals.

institutions and online marketplaces facilitating those sales may incur substantial damage to both reputation and revenues.

While the sale of counterfeit goods is by itself criminal, this activity is often linked to other more serious crimes, ranging from money laundering and extortion to funding criminal or terrorist organizations.

According to the **UNODC,** the involvement of organized crime groups in the global production and distribution of counterfeit goods is on the rise. Not only do criminal organizations use funds from other illicit activities to finance their counterfeiting operations, but also vice versa. They use similar methods to traffic counterfeits as they use to move illegal drugs, firearms and people trapped in human trafficking schemes.

In its latest **Review of Notorious Markets for Counterfeiting and Piracy,** the US Trade Representative (USTR) noted that factories producing counterfeit goods are indeed partially driven by forced labor and human trafficking.

To combat this vicious cycle, regulators and card schemes are committed to imposing severe penalties on marketplaces or financial institutions facilitating those transactions. For instance, the US introduced the **INFORM Consumers Act in 2023,** which requires online marketplaces to implement higher levels of seller verification and offer mechanisms for consumers to report suspicious seller activity.

▸ Learn more about the risks entailed in counterfeiting **here.**

## Prohibited Adult Content

With the continued advancement of smartphones and Wi-Fi accessibility, the ability for users to upload adult content to the internet has become easier than ever.

Platforms and merchants providing access is legally permissible, however authorities require that significant controls be in place to monitor, block, and remove all illegal content. Not only do such practices help protect internet users, the online purchase or trade of illicit media is a known contributor to sexual and human exploitation and the spread of transnational crime.

Card schemes thus maintain close partnerships with law enforcement to expel prohibited adult content from online circulation.

> Throughout 2022, 9% of all notifications issued to EverC clients fell within this high-risk category.

This included flagging merchants with possible connections to media or services involving illicit content such as non-consensual sexual condut, bestality, etc.

In 2021, major card brands have introduced additional requirements for financial institutions and platforms processing payments for adult content to ensure that they implement strong control measures. By registering an adult content and services merchant, or sponsored merchant (MCC 5967), acquirers certify that they meet certain requirements and maintain effective controls to monitor, block and possibly take down all content as appropriate.

In the case that some merchants allow a third-party user (“content provider”) to upload or generate content, including real-time/live streaming content, both entities must ensure the following:

- Specifically prohibit illegal or otherwise violative content
- Age and identity verification
- Content review and reporting
- Confirm the consent of the parties involved

Merchants must also provide a mechanism for which users can file complaints or for any person depicted to remove content. In the case of Mastercard, these security rules and procedures were updated as of February 2023 **(Sec 9.4.1)**.

Imposing stricter compliance rules was partially motived by **claims of sex trafficking and child exploitation** facilitated by popular adult content platforms, such as Pornhub, in 2020. To which, a review of the website uncovered unlawful content on the site, particularly relating to content depicting minors.

Unfortunately, the proliferation of illegal adult content will continue to plague the internet for the foreseeable future. It is the responsibility of every participant in the payments ecosystem to actively disrupt bad actors from profiting off such illicit activity.

## Illegal Gambling

Gambling is a regulated industry in many jurisdictions, including when conducted online. The fact that it is also prohibited in several regions further complicates efforts to combat illegal gambling and the entry of illicit merchants and transactions into the payments system.

Just like how cash-heavy casinos have been traditionally used by organized crime networks, fraudsters use online gambling to launder money and carry out other financial crimes in a variety of ways. Many gambling sites don’t maintain effective AML

protocols, making them attractive targets that offer criminals multiple avenues to funnel illicit funds through the system. This includes the quick cash-in cash-out tactic, underground banking (known as **Hawala**), collusion between players, or using gambling accounts to facilitate illegal transactions, such as purchasing real estate or other expensive assets.

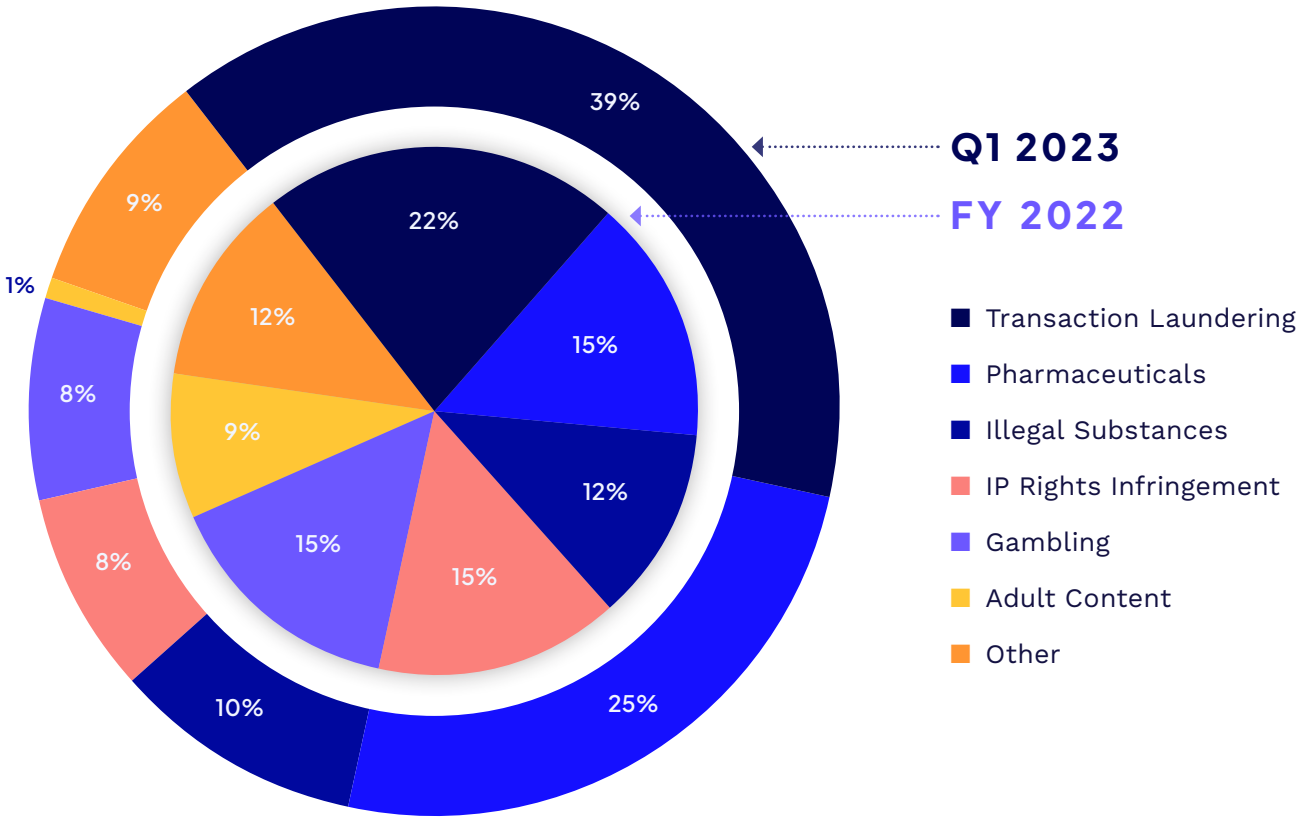
EverC solutions categorize gambling violations as merchants dealing in paid gambling services such as casinos, poker, lottery bingo, etc. In this context,

> 15% of all notifications in 2022 pertained to gambling violations.

However, card schemes may also consider cryptocurrency, binary options, security brokers, and other operations as indications of risky behavior.

Acquirers and partnering financial institutions are required to identify gambling transactions with correct MCCs and Point-of-Sale Condition Codes. However, many fraudsters will often intentionally miscode online gambling transactions to circumvent card scheme requirements and launder their funds.

# Global trends to watch for in 2023




Illicit actors in ecommerce are constantly evolving. But at EverC, our team of experts works with our proprietary technology to stay ahead of bad actors. Now that EverC industry experts have compiled data from our investigative findings in 2022, we can draw certain conclusions and analyze what this can mean for fraudulent behavior, trends, and tactics.

For instance, as demonstrated by data compiled from the first quarter of 2023, there are clear indications that these trends will continue to plague the payments industry in the coming year. This is particularly concerning the top five types of violative behavior recorded: Transaction laundering, illicit sales of pharmaceuticals, illegal substances, IP rights infringement and gambling.

**Let's take a deep dive into trends to look out for in 2023.**

## Transaction Laundering

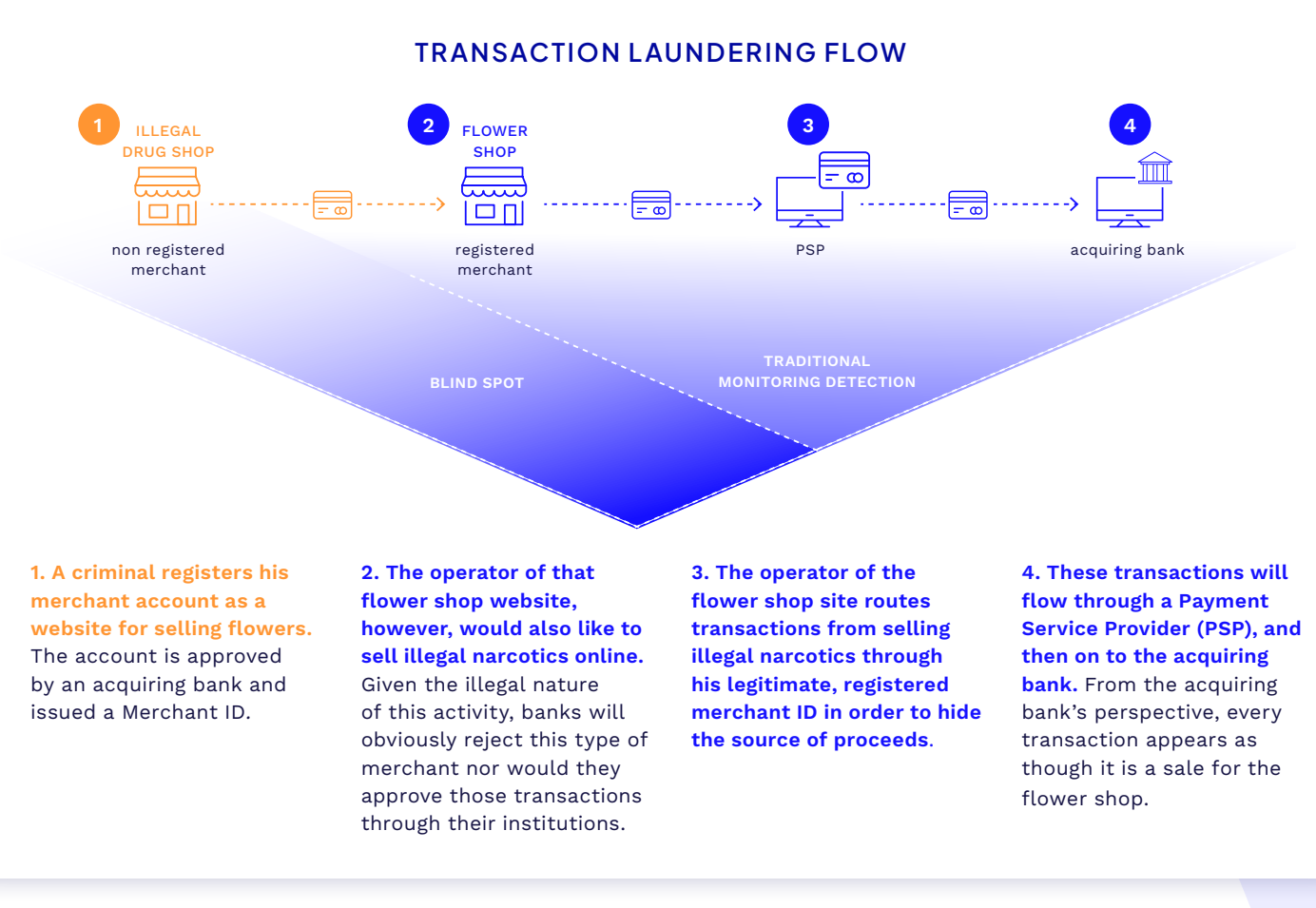
Transaction laundering is an advanced fraud scheme that puts the global financial network at risk.

> This was the most common method for illicit payments activity detected among EverC clients in 2022 and in the first quarter of 2023, accounting for 22% and 39% of notifications, respectively.

Criminals operating websites with the objective of transaction laundering will use approved merchants to process payments on behalf of another entity unknown to the acquirer or payment provider, thus violating the merchant's agreement with the latter.

In essence, the traditional "carwash" method of cleaning cash moved online and uses various types of front entities to launder money. This can include front companies, pass-through companies, or funnel accounts procuring payments and reintroducing illicit funds into the financial system.

**This image showcases a step-by-step flow of transaction laundering operated through a front website**




**1. A criminal registers his merchant account as a website for selling flowers.** The account is approved by an acquiring bank and issued a Merchant ID.

**2. The operator of that flower shop website, however, would also like to sell illegal narcotics online.** Given the illegal nature of this activity, banks will obviously reject this type of merchant nor would they approve those transactions through their institutions.

**3. The operator of the flower shop site routes transactions from selling illegal narcotics through his legitimate, registered merchant ID in order to hide the source of proceeds.**

**4. These transactions will flow through a Payment Service Provider (PSP), and then on to the acquiring bank.** From the acquiring bank's perspective, every transaction appears as though it is a sale for the flower shop.

As transaction laundering activity falls outside the scope of more established monitoring protocols of the traditional banking sector, the practice represents a major blind spot for acquirers and financial institutions. It is nearly impossible for risk and underwriting departments in the payments ecosystem to maintain pace as transaction laundering operations continue to spiral upward in speed and sophistication.

As a known method to facilitate a range of financial crimes, the impact of transaction laundering is not limited to the operations and reputation of stakeholders in the payments ecosystem. The anonymity provided by transaction laundering also enables criminals to maintain fraud rings across the globe, many of which have been connected to human trafficking rings or shown to support terrorist organizations.

Authorities and card brands have therefore expanded their transaction laundering detection capabilities in recent years. However, the ease at which criminals can create a fraudulent website indicates that this will continue to be a favored method for the foreseeable future.

▸ Learn more about transaction laundering by reading our whitepaper on the topic **here**.

**Other prominent threats have been troubling the payments ecosystem for a while, and potentially escalate through 2023.**

## Cryptocurrency Scams

Cryptocurrencies are digital tokens that can be sent electronically from one user to another anywhere in the world. Unlike traditional payment systems, decentralized networks of computers keep track of all cryptocurrency transactions, allowing for greater anonymity reinforced by the blockchain technology it uses.

For criminals, this makes cryptocurrency much more attractive than other payment systems, which generally require customers to provide identification before opening an account and making transactions. According to leading blockchain intelligence company **Chainalysis,** hackers stole nearly $3.8 billion from cryptocurrency businesses in 2022, up from $3.3 billion in 2021 and a significant jump from $500 million in 2020.

Indeed, a range of crypto hacking and company mismanagement scandals dominated financial news coverage in 2022. Most notably, the **collapse of the FTX crypto exchange platform** lost users nearly $8 billion of investor money in what US prosecutors called “one of the biggest financial frauds in American history”. While this was the most famed in a series of schemes that defrauded investors out of billions, it shined the spotlight on crypto investment scam operations and the risks posed to consumers.

Pig butchering is another scam that has been **making headlines** in recent months. Based on the term for fattening a pig for slaughter, this modern version of a romance scam is swindling millions from unsuspecting victims around the world. Scammers create fake online dating profiles and then groom their targets to invest in cryptocurrencies through sham websites controlled by their accomplices. Once victims invest enough money, the scammers take it all and vanish.

On a broader level, criminals seeking to launder money or scam victims often combine methods to accomplish their goal.

Crypto scammers use complex and deceptive techniques to steal funds from their victims and move them across organizations in the payments ecosystem. Furthermore, dealings with cryptocurrencies have proven to be used in a range of illicit activities, from small-scale scams and identity theft to money laundering and human trafficking.

As authorities take progressive steps to make cryptocurrency regulations stronger, the ecommerce space will continue to see a wide range of high-risk activity. And payment providers may indeed be held liable for crypto scams laundered or transacted through their services.

▸ Learn more about this super scam by reading our whitepaper on the topic **here.**

## Here's how funds from cryptocurrency-related crime can be procured and reintroduced into the financial system

### 1. CRYPTOCURRENCY EXCHANGES

**a.** Criminals deliberately seek out exchanges that have weak or no KYC requirements.

**b.** These exchanges are used in jurisdictions that may not be regarded as high-risk for crypto asset laundering.

**c.** Criminals present fraudulent documents, or use money mules, at legitimate exchanges to add credence to their operations.

### 2. PEER-TO-PEER PLATFORMS

Depending on their jurisdiction, some P2P platforms may not be subject to KYC regulations, allowing criminals to engage in illicit transactions without the involvement of centralized intermediaries

### 3. DECENTRALIZED EXCHANGE SERVICES (DEX)

Criminals can bypass compliance controls by making real-time crypto asset exchanges using a DEX, which lacks a central administrator with oversight of user accounts, records, or identities.

### 4. CRYPTOCURRENCY ATMS

Largely unregulated across the globe, criminals use these to convert large amounts of cash into cryptocurrencies, or vice versa.

### 5. ONLINE CASINO AND GAMING SERVICES

Criminals exploit lacking KYC protocols of many sites to swap cryptocurrencies for credits or in-game currencies to clean their illicit funds.

### 6. PRE-PAID CARDS

Criminals load pre-paid cards with illicitly procured cryptocurrency to make purchases or swap it with fiat currency.

### 7. MIXING SERVICES AND PRIVACY WALLETS

Allows criminals to operate with increased anonymity as these services break the chain of end-to-end traceability around cryptocurrency transactions.

### 8. TOKENS

Criminals can purchase tokens without providing identifying information and clean illicit funds.

## High-Risk Jurisdictions

High-risk jurisdictions have strategic deficiencies in their national AML/CFT regimes, posing a risk to the international financial system. These are mainly designated by the Financial Action Task Force (FATF), which identifies these jurisdictions and stipulates recommendations based on internationally endorsed global standards against money laundering and terrorist financing.

▸ The FATF review process for high-risk and other monitored jurisdictions can be found **here.**

In regions where AML/CFT procedures are weaker, higher levels of financial crime and corruption are recorded. Any financial institution seeking to enter into a business relationship with a person or entity established in a high-risk jurisdiction must therefore implement Enhanced Due Diligence (EDD) measures. This is part of adopting a risk-based approach within compliance programs to mitigate financial crime risk.

Additionally, financial institutions need to be aware of the possibility of sanctions when dealing with certain jurisdictions or politically exposed persons (PEPs), both of which constitute an elevated risk. Despite the vast majority of AML/CFT frameworks including prohibition of dealing with sanctioned individuals and businesses, preventing cross-border transactions or the sale of products to/from sanctioned entities is a complex challenge.

For example, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) enforced action against a US cosmetics company that supposedly purchased false eyelashes from two China-based suppliers, 80% of which contained materials sourced from North Korea over the course of a five-year period.

OFAC highlighted that the company did not exercise "sufficient supply chain due diligence" while sourcing products from China, which is "a region that poses a high risk to the effectiveness" of North Korean sanctions. In this case, the company should have conducted supply chain audits to verify the country of origin of goods and services and adopted new procedures requiring suppliers to certify compliance with US sanctions.

On a broader scale impacting multiple players in the global payments system, we can examine the tranche of sanctions imposed against Russia for its ongoing military incursion into Ukraine. A host of high-risk and illegal activity was subsequently recorded as Russian financial institutions and linked entities sought to evade sanctions through a variety of avenues, including the creation of trusts, shell companies, or use of pooled investment schemes. Shortly after the conflict began, the US Financial Crimes Enforcement Network (FinCEN) issued its first in a series of **alerts** urging all financial institutions to be vigilant of Russian-perpetrated financial crime.

Every player in the payments ecosystem with a correspondent nexus to Russia is now under pressure to review their sanctions compliance protocols. Stricter protocols prohibit new investments, the export or sale of goods, services, technology, financing facilitation, and guarantees; any individual or entity found to be facilitating any of these activities would be subject to significant penalties or even arrest.

Requirements and enforcement actions are more prominent in the financial services and payments industry, but it's important to remember that other sectors also receive serious fines and penalties for non-compliance. This is why enhanced due diligence and monitoring protocols, sometimes performed by third parties, must involve checking sanctions lists targeting individuals, countries, groups, or companies.

## Other threats to consider

Fraudsters will continue to change their attack patterns. As technology evolves, so do those who exploit it for ill-gotten gains. Companies will need to pivot from traditional security protocols and fraud prevention methods to navigate the rapidly expanding threat landscape.

**SuperApps,** for example, are quickly redefining digital ecosystems on a global scale. The expected popularity and rapid development of these one-stop-shop applications, including from the likes of giants such as **Twitter and Walmart,** make them a prime target for criminals to conduct a range of fraudulent activities. The more services an app offers, the larger the attack surface it creates for fraudsters to infiltrate. (If your data is stolen or leaked by one app, the situation can more easily be contained to the one app. If it's compromised in a super app, it affects countless other apps you rely on for your daily life.)

Another challenge facing 2023 is the **rise in Synthetic ID fraud**. While traditional identity fraud typically means that a criminal steals and misuses a person's actual identity, synthetic ID fraud occurs when criminals combine fake and real identification information to create a completely new identity. Using fabricated data makes it even more difficult for authorities to identify a fraudster, with some cases of Synthetic ID fraud going undetected for years.

Synthetic ID fraudsters often target minors. In the US, children hold valid social security numbers but don't have credit or credit history, so guardians and authorities don't pay much attention to their financial activity. Following a staggering loss of about $20 billion for US banks and financial institutions in 2020 alone, the US Federal Reserve released a **Synthetic Identity Fraud Mitigation Toolkit** to support the payments industry in eradicating this criminal practice.

## Regulatory response

Despite efforts from authorities to combat illicit financial crime around the world, criminals have demonstrated their capacity to adapt and reinvent ways to reach their goals. The **UNODC** estimates that the amount of money laundered in one year is 2-5% of the global GDP, or $800 billion to $2 trillion USD. From IP infringing products and services to illegal pharmaceuticals, the proceeds of financial crimes are clearly being reintroduced into the payments system on a continuous basis, posing extensive risks to financial institutions facilitating those transactions.

To meet the challenges of this increasingly complex financial landscape, authorities across the world have been working to tighten gaps in AML legislation.

For example, there is an increasing regulatory focus on **Buy-Now-Pay-Later (BNPL).** BNPL products are an alternative to traditional credit, providing users with interest-free finances. BNPL providers buy the value of goods or services from merchants and then collect repayments from consumers in installments, all while earning fees for transactions.

In the UK, complaints against BNPL firms **increased 36 percent** in the past three years, leading regulators to launch a **consultation** to strengthen BNPL legislation in February. Similarly, Australia seeks to include BNPL under the **National Consumer Credit Protection Act.** In the US, increasing oversight on the BNPL sector has been on deck since 2021. In the coming months, the Consumer Financial Protection Bureau (CFPB) plans to **issue guidance** for BNPL vendors in order to continue operating under existing credit card protections laws.

Regulators will not be easing off their heightened focus on combating global financial crime any time soon. Adding to the fact that card schemes maintain their own set of AML rules and guidance, often backed by law, we see a scenario in which players within the payments ecosystem will be compelled to review and strengthen their AML protocols.


Here are some of the most prominent AML regulations slated to take effect in the near future
The US INFORM Consumers Act will require online marketplaces to implement higher levels of seller verification and offer reporting mechanisms for consumers to report suspicious seller activity (June 27, 2023)
The EU's Anti-Money Laundering Authority (AMLA) is scheduled to be operational as part of updates to its Sixth Anti-Money Laundering Directive (2024)
China is in the midst of a Three-Year Action Plan for Combating Money Laundering Violations and Crimes to strengthen its existing AML framework. This crackdown on financial institutions will make compliance requirements more rigid and strengthen AML/CFT investigation protocols (until December 2024)
The EU's Markets in Crypto Assets (MiCA) framework to regulate unbacked crypto assets and stablecoins. This will require crypto service providers to implement KYC protocols and sanctions screening processes (2024)
The UK's Second Economic Crime (Transparency and Enforcement) Bill will include new regulatory powers to recover crypto assets derived from financial crimes, introduce a beneficial ownership register of foreign entities owning property in the UK, and enhance existing AML regulations (Several deadlines slated in 2023)
The US Enablers Act would expand the Bank Secrecy Act's definition of "financial institution" by placing new requirements on various players who have a part in facilitating transactions (to beresubmitted to Congress in 2023)
Under the US Corporate Transparency Act, FinCEN's "Final Rule" will come into force requiring individual and foreign organizations to report their true beneficiary information (January 1, 2024)

# Summary


KEY TRENDS TO WATCH FOR IN 2023
**Scams targeting Super Apps** to maximize potential payouts due to highly connected data
**Synthetic ID fraud** combining authentic and counterfeit information to make detection more difficult
**Super scams, such pig butchering,** using crypto to steal, launder, and hide funds
**Continuing use of transaction laundering** to funnel money to larger criminal networks
**Higher levels of online financial crime** originating from high-risk or sanctioned jurisdictions
**Increased scrutiny from global regulators and card schemes,** to protect consumers from all of these threats

# Conclusion

## Technology: A tool to fight fraud

Fighting fraud and maintaining compliance in an ever-evolving threat landscape is an expensive proposition, but ignoring has an even higher cost. **Financial institutions were reportedly fined nearly $5 billion USD** for anti-money laundering violations, breaches of sanctions, and flaws in Know Your Customer (KYC) protocols last year.

For businesses that rely on safe, secure, scalable ecommerce, the challenge continues. Payment providers and marketplaces will need to step up efforts to combat the unified threat landscape. Ongoing problems will continue to spiral up. New scams will continue to proliferate. And there will be intensified regulation and investigation to meet these escalating threats.

Organizations are quickly adopting artificial intelligence to help detect potential fraud: 77% Share of FIs that report using AI systems to detect transaction fraud (PYMNTS report). Machine learning is essential to the task of monitoring the sheer volume of data, identifying the rapidly changing tactics of illicit actors, and providing the evidence to support the next steps, whether they include removal or remediation of merchants.

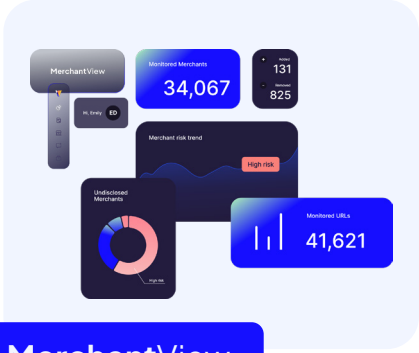
Investing in comprehensive compliance programs is a critical step for payment providers to address risks and ensure that they are following the law, protecting their business and brand from enforcement action that can carry both monetary and reputational consequences, and joining the fight against financial crime.

# Partnering with EverC

EverC technology can empower risk and compliance teams with actionable intelligence to make more nuanced, evidence-based decisions. EverC is focused on powering growth for the ecommerce ecosystem. Our automated AI-driven, cross-channel risk management solution rapidly detects high-risk merchants, transaction laundering, and illicit products, and provides ongoing monitoring to uncover evolving risks. Our team comprises domain experts in risk intelligence, open-source, deep and dark web, and online fraud detection.

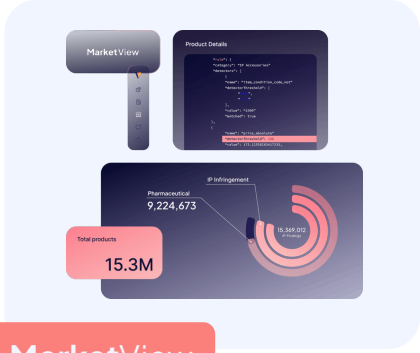
Our solutions combine artificial intelligence with expert insights, for fully integrated, customizable merchant and marketplace risk management.

EverC solutions and services provide actionable intelligence: A holistic view of the collaborative threat landscape that enables us to take down entire networks of illicit actors for safer, more successful ecommerce.




**MerchantView**

Merchant risk intelligence platform that uncovers money laundering and additional risk factors.




**MarketView**

The only fully automated solution that identifies and eliminates illicit and counterfeit products.


**Risk Insight Services**

Our global experts provide investigation services tailored to your risk and compliance needs.

**EverC: securing ecommerce growth with trust and confidence**

Learn more at **everc.com**