THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

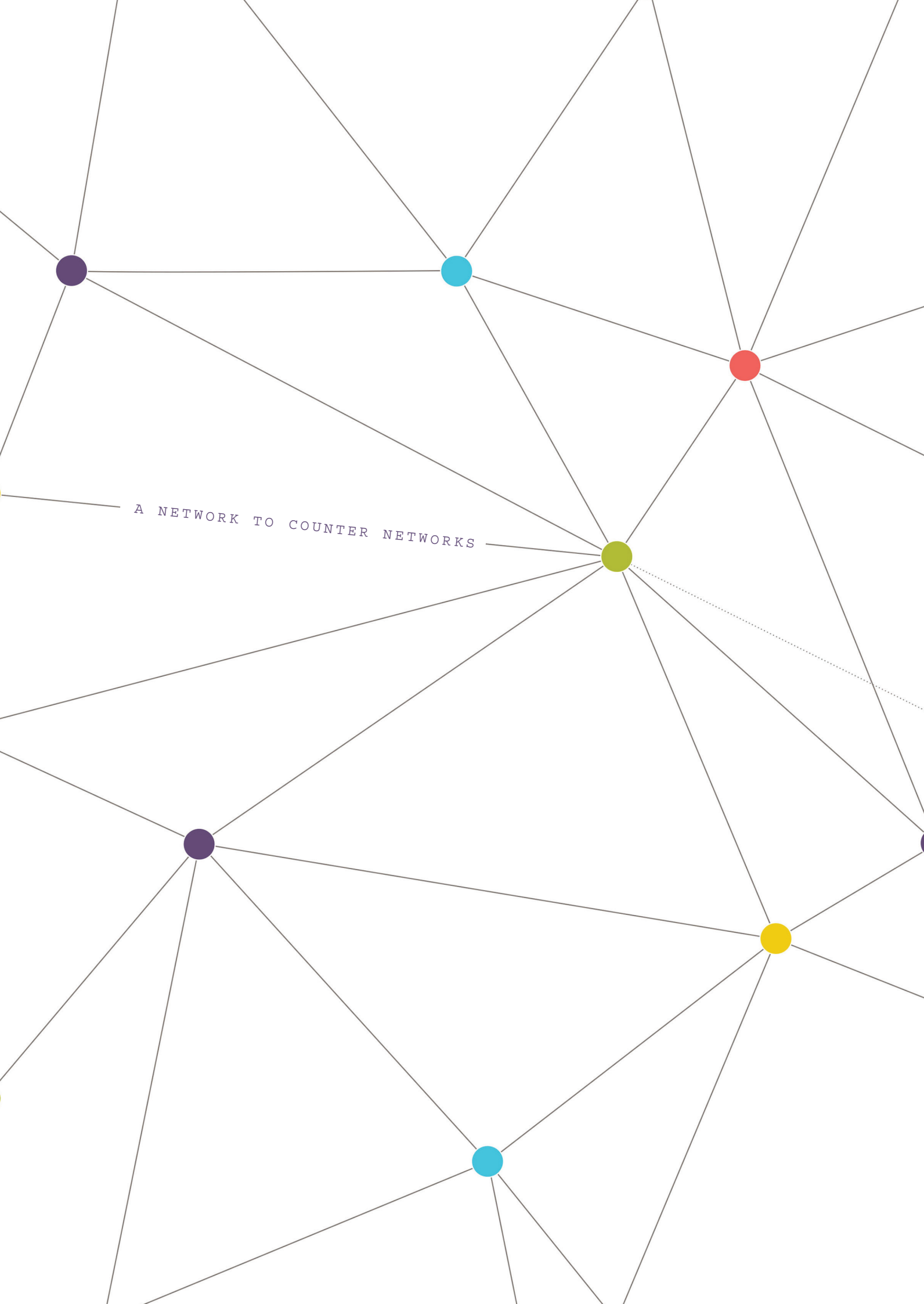
DIGITAL DANGERS

CUT THE PURSE STRINGS

Rupert Horsley

Targeting the online illegal wildlife trade through digital payment systems

May 2018


A NETWORK TO COUNTER NETWORKS

CUT THE PURSE STRINGS

Rupert Horsley

Targeting the online illegal wildlife trade through digital payment systems

May 2018

Cover photo: iStock/lara_zanarini

The Global Initiative Against Transnational Organized Crime
WMO Building, 2nd Floor
7bis, Avenue de la Paix
CH-1211 Geneva 1
Switzerland

www.GlobalInitiative.net

Contents

Summary

There has been startling growth in the online illegal wildlife trade (IWT), and broad recognition of the need to apply financial and anti-money-laundering tools to the fight against environmental crime. Much illicit trade carried out over the internet requires some form of electronic payment. This paper explores how various payment methods are used in the online IWT, and the challenges and opportunities these present to law enforcement. Some inroads have been made into combating the online counterfeit trade by suppressing activities of 'rogue' digital payment providers that facilitate illicit trade. Opportunities to target the online IWT by monitoring digital payment transactions will emerge only if regulatory systems and technology keep pace with levels of innovation used by illegal wildlife traders to avoid detection.

Key points

- The dynamic growth and fractured nature of online payment systems present considerable challenges to law enforcement and regulators across all sectors.
- The online IWT varies across region and product type. Traders have been found to make use of various payment methods, at least in part reflecting concerns about privacy and security. These include e-wallets or payment intermediaries and direct deposits. Card payment systems, traditionally the dominant force in digital payments, are also likely to be used.
- Reflecting broader regional trends, researchers have identified the use of e-wallets, such as WeChat Pay, in the online IWT in China and other Asian countries. Until recently, e-wallet payments have been somewhat opaque in China. However, the creation of a new clearing house for all non-bank intermediaries in the country may offer opportunities for collaboration in the bid to deny traders the use of such payment services. Models for this exist in the fight against the online counterfeit trade.
- There has been no significant uptake of crypto currencies in the online IWT. There is also limited evidence that cash on delivery or mobile money is being used to any great extent.
- Attention should be paid to developments in online payment system technologies and the efforts of regulators to keep up with these, particularly in Asian markets such as China and Malaysia, where innovation is most concentrated. As new regulations are adopted, opportunities to deny online traders the use of payment services are likely to emerge.

Introduction

With the growing recognition that illegal trade in wildlife is a major organized transnational crime – as opposed to just a niche conservation concern for environmentalists – attention has been turning to the need to use anti-financial-crime and anti-money-laundering tools to fight this global scourge.

Starting with the London Conference on the Illegal Wildlife Trade in 2014,[1] a series of international events (Kasane in 2015 and Hanoi in 2016) have called for the financial aspects of the IWT to be included in the global response. Acknowledging the progress already made, the Hanoi conference welcomed the inclusion of the IWT on the agendas of such international organizations as the Financial Action Task Force, INTERPOL, the UN Office on Drugs and Crime, the World Bank and the World Customs Organization.[2] Reinforcing the growing focus on the financial flows of this illegal trade, the UN General Assembly has called for member states to make it a predicate offence (the designation for a crime underlying money-laundering offences) and to use legal instruments, such as the UN Convention against Corruption, to combat it. Environmentalists are lobbying to the same end.[3]

While the use of these traditional mechanisms is vital to combating the global growth of the IWT, the specific characteristics of online IWT may require additional, less conventional approaches. Along with other illicit trades that have flourished on the internet, illegal wildlife trading is able to take advantage of an ever-proliferating array of platforms and electronic payment methods with which traditional law enforcement and financial regulations struggle to keep pace.

Furthermore, the complex landscape of electronic payments outlined here is compounded by a lack of clarity about exactly who is participating in the online IWT. Evidence gathered in investigations so far suggests the presence of transnational networks, sending, for example, large quantities of ivory from Japan to China,[4] domestic traders with access to substantial stocks of wildlife products,[5] and individual retailers whose small transactions nonetheless aggregate into significant quantities.[6] There is also evidence that bigger dealers use agents to retail their products. In one such identified system for the online ivory trade in China, agents post information about products for sale, and when they attract a buyer they purchase the product from the main dealer and resell it for a profit.[7]

Given the great variety of available payment methods, and the different trading arrangements and networks that exist to bring wildlife products to the online market place, targeting traders through their financial flows is a daunting challenge. However, e-commerce of any significant scale must ultimately rely on a network of financial institutions to send and receive payments, and targeting traders' access to these might make such activities considerably less appealing to criminals.

In this briefing, we aim to sketch out the dynamic landscape of online payment systems with reference to the IWT and explore some of the challenges and opportunities facing regulators and law enforcement. We conclude with a brief account of initiatives in which online payment systems are being used to curb the online counterfeit trade, in the hope that this may offer models that could inform the response to the online IWT.

Acknowledgements

The authors would like to thank the Government of Norway for funding this report. Digital Dangers forms part of a partnership project between INTERPOL and the Global Initiative Against Transnational Organized Crime, in cooperation with the UN Office on Drugs and Crime.

The growth of online IWT

In line with the global growth in internet usage and e-commerce, the illegal wildlife trade has increasingly moved online over the past decade, and the internet is now recognized as a key front in the global battle against environmental crime. E-commerce holds various attractions for wildlife criminals. In particular, it enormously expands the potential markets that traders have access to while, simultaneously, increasing anonymity and lowering risk. Recognizing these developments, the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) has adopted various decisions in the area of combating wildlife cybercrime.[8]

A key challenge when it comes to formulating responses to online IWT is its huge diversity across platforms, regions and products. The most active markets in Europe, Asia and the US have taken to the online space in different ways, and the goods offered for sale vary considerably, from a thriving trade in live pets in the Middle East to ivory and traditional medicine in China – with much in between.[9] Online wildlife traders can also choose from a host of platforms to market their products, including large e-commerce companies, such as eBay or Alibaba, classified websites, specialist forums and auction houses, and social media.

Although we still have only a limited understanding of how online wildlife traders operate and interact with one another (for example, it is not obvious how to differentiate between organized gangs and individual retailers on the internet), investigations and interventions have steadily grown in intensity over the past decade, with large e-commerce companies actively seeking to suppress IWT taking place on their platforms.[10]

These efforts have had a significant impact on illegal wildlife trading on major online marketplaces.[11] However, these successes in suppressing IWT on large e-commerce platforms have, in many cases, led traders to migrate to areas of cyberspace that offer greater privacy and anonymity, such as closed forums and social-media groups.

The huge variety of such platforms available to online wildlife traders means that monitoring and removing advertisements alone will not be enough to end the trade. Alongside these efforts, there is a recognized need for research into how the financial flows that accrue from the IWT pass through online payment systems, which may offer additional, more durable means of disruption.

The online payment ecosystem

Unfortunately, the landscape for digital payments is growing massively in scale and complexity, creating an ecosystem that is challenging to monitor. Along with the card payment system (i.e. credit cards and debits cards), which has traditionally dominated payments in e-commerce, online traders can now choose from a variety of options for making direct deposits and a proliferating array of payment intermediaries and e-wallets (see Table 1 for a summary). This is not to mention mobile money, cyber currencies and the enduring popularity of cash on delivery in less-developed markets.

These payment systems are integrated with the regulated global financial systems to differing degrees, allowing criminals to move money in ways that are difficult to trace. Their popularity and uptake also vary widely across the globe, complicating efforts to forge a comprehensive response.

Noting the challenge posed by the growing complexity of online payment systems, in particular the emergence of payment intermediaries that do not have uniform rules or regulatory frameworks and which can offer transfers between different intermediaries or from peer-to-peer, the World Bank concludes that anti-money-laundering measures that were implemented to fight illicit transfers fail when it comes to most digital payment providers. Moreover, a payment intermediary can always benefit from the differences in regulation between various

jurisdictions and choose a less regulated environment while being able to operate all over the world through global information networks.[12]

Addressing this issue regarding the IWT specifically, TRAFFIC acknowledges that the dynamism of online payment systems and the speed of transactions are major obstacles to monitoring the online IWT and enforcing the law.[13]

Despite this rather bleak outlook, and the lack of research focused specifically on the payment systems used across the range of online IWT, some of the services favoured by traders are inherently traceable, and there are signs that regulators will eventually find ways of bringing the field under closer scrutiny.

Table 1: Types of digital payment systems

Payment type	Nature and regulation
E-wallets and payment intermediaries	Diverse field, including PayPal, WeChat Pay, Alipay, Google Pay, etc. Smaller providers are also proliferating enormously in domestic markets. Regulatory oversight varies. PayPal has established anti-money-laundering policies and claims to comply with all applicable regulations; Chinese e-wallets are being brought under closer regulation by the Online Settlement Platform for Non-Bank Payment Institutions. Domestic regulations elsewhere vary.
Card payment networks	Dominated by the Visa and MasterCard networks. Prominent in Western digital markets, the networks impose their own policies on participating banks and comply with financial regulations.
Direct deposit	Payments between banks via computer networks such as ACH in the US and SEPA in the EU. Subject to financial regulations in the respective regions.
Crypto currencies	Largely anonymous currency based on blockchain technology. Minimally regulated at present.
Mobile money	Popular in sub-Saharan Africa. Allows users to transfer credit on mobile phones between service providers or individuals without the need for a bank account. Users can be identified by their mobile accounts, and transaction sizes are limited.

E-wallets and payment intermediaries

E-wallets and other financial intermediaries are a popular form of online payment, particularly for international transactions. The UN Conference on Trade and Development (UNCTAD) cites a survey of e-shoppers in 26 countries showing that e-wallets were the preferred method of payment for 41 per cent of participants (compared to 33 per cent for credit cards, and 18 per cent for debit cards/bank transfer).[14]

While PayPal is perhaps the best known e-wallet in the West, in China, which is widely considered the most active and innovative market for e-payment systems, there are a large number of competing e-wallet companies. The Chinese market is dominated by Alibaba Group's Alipay and Tencent's WeChat Pay. The latter, which is offered on the hugely popular WeChat messaging platform, has been identified in various investigations as a preferred method of payment in the online IWT.

How does it work?

E-wallets work in a variety of ways, with the term often being used as a catch-all for intermediaries that process payments in a number of ways. For example, e-wallets can make use of debit or credit cards, simply sitting between existing nodes in the card payment system; they can link directly to a customer's bank account; or they can use balance directly uploaded from customers' bank accounts to the e-wallet. Which system is favoured depends on the region and the provider. One industry analyst estimated that 30 to 50 per cent of PayPal transactions involve a credit card, whereas in the case of e-wallets in China, where direct linkage to bank accounts is preferred, the proportion is probably very minimal.[15] On top of this regional variety, the dynamism of the global market for online payment services means that there is not a clear picture of who all the players are. For example, in Malaysia alone one report anticipates 10 new e-wallets being established in 2018.[16] Moreover, while big players, like PayPal, have developed anti-money-laundering procedures, many of the other service providers do not have effective checks in place.[17]

Visa and MasterCard, which sit behind most e-wallet payments that use credit or debit cards, channel all transactions through their own networks. This facilitates monitoring and regulation. Payments that use e-wallet balances, or in which e-wallets are directly linked to bank accounts, however, can be more fractured and opaque. For example, in China the system is primarily based on bilateral relationships between banks and e-wallet providers, with the e-wallet companies holding all financial data themselves. Banks do not receive any information on the name or location of the recipient of the funds, only the name of the e-wallet provider.[18]

This fractured system hinders monitoring and investigation – a particular problem given the identified role of e-wallets in the IWT in Chinese and other Asian markets. However, the Chinese government has made moves to centralize the system, while the international growth plans of WeChat are pushing them to embrace card payments (see below).

WeChat Pay and IWT

Investigations into the use of social media and online forums by those engaging in the online IWT have recorded numerous instances of traders favouring e-wallets for transactions, in particular the various payment systems offered by Tencent's WeChat, such as WeChat Pay.

An investigation by TRAFFIC into the use of social media in China's illegal ivory trade, for example, published in 2015, found that WeChat was a highly popular messaging platform and WeChat Pay was traders' favourite payment method, in part due to perceived convenience and privacy.[19] Notably, this investigation also revealed that traders could be choosy about which online payment services were used, refusing to accept payment through a provider called 'Zou Bao' out of fear that law-enforcement agents were using it to entrap traders.[20]

WeChat payment services have also been recorded in cross-border online trade. An investigation by the Wildlife Justice Commission (WJC) into the illegal wildlife trade in the Vietnamese village of Nhi Khe, which began in 2015,

found that Chinese customers use WeChat wallets to transfer funds to Vietnamese traders.[21] Interestingly, the WJC said that the scale of the trade uncovered and the number of products being offered by a small group of traders suggest that this method is used by organized networks.[22]

What isn't clear from the research is whether WeChat Pay (or other payment services) is being used, in these instances, with payment cards or through direct linkages to bank accounts. In the circumstances, it may well be likely that traders would opt for the latter, more discreet, method.

Increasing regulation

Although e-wallets have been found to be popular payment methods with traders in the online IWT, partly because of the perception that they are relatively private, there is reason to believe that the situation – in China, at any rate – is changing.

Most importantly, in August 2017 the People's Bank of China sent a letter to all third-party payment providers in the country requiring them to register with a clearing house, called the Online Settlement Platform for Non-Bank Payment Institutions, by October that year, and to channel all payments through the clearing house by June 2018.[23] This directive affects Tencent payment services, Alibaba Group's payment services, and all other e-wallets operating in China. With all transactions being made via the clearing house, the People's Bank of China will now be able to directly monitor transactions without having to request information from the service providers. This will aid in the detection of money laundering and illegal payments, including those made to procure wildlife products.

Another development that may be significant is the expansion of WeChat Pay to markets outside China. Previously a Chinese bank account was required to use WeChat Pay services. However, Tencent now allows linkage with international credit cards provided by Visa, MasterCard and JCB to expats living in China and residents of Hong Kong, Macau and Taiwan.[24] WeChat Pay has also been established in South Africa for some years. Although these developments may facilitate international transactions for online wildlife traders, the integration of WeChat Pay with the card payment system may also enable easier regulation of these financial flows.

Guaranteed transactions

Noting the need for trust in the movement of funds related to the online IWT, TRAFFIC has said that guaranteed transaction services are increasingly being employed in the IWT and calls for them to be tracked as a means to interdict online wildlife trade transactions.[25]

How does it work?

With guaranteed transactions, the buyer of a certain product transfers the payment to a trusted intermediary. When the intermediary confirms that the funds have been received, the seller sends the product to the buyer. The buyer now instructs the intermediary to release the funds to the seller, and the transaction is complete. Such mechanisms are commonly used in complex and high-value transactions, for example those involving property developments and business deals, and they are an important reason behind the growth of online markets. Such services are offered by e-commerce platforms and e-payment services, such as e-wallets. As an important example, Alibaba's Alipay offers a guaranteed transaction service that is credited with facilitating the huge growth of e-commerce in China[26] and is used by 68 per cent of all online shoppers in China.[27]

If it is indeed the case that guaranteed transaction services are increasingly being used in the online IWT, then targeting these service providers and denying traders access to them could be an effective means of disrupting the illicit trade, particularly in retail where a lack of trust is greatest (organized networks trading in large volumes presumably trade off trust that is already inherent in their relationships).

At present, there is little research into what guaranteed transaction services are being used in online IWT, where, and by whom. However in one notable finding, the Project to End Great Ape Slavery (PEGAS) recently published an article detailing the widespread use of private guaranteed transaction services for the online trade in apes in Indonesia.[28] Referred to as 'rekber', these typically involve a private service provider making use of traditional banks to act as the guarantor of the transaction for a fee. As PEGAS notes, this arrangement suggests that Indonesian banks are unwittingly facilitating the illegal wildlife trade.

It is not clear from current research to what extent the guaranteed transaction services offered by large companies, such as eBay, Alibaba and Tencent, play a part in facilitating the online IWT. Notably, while TRAFFIC has raised this as a potentially important area for disruption, it has also revealed that some traders in the illegal online wildlife trade in China are wary of using the guaranteed transaction services offered by online payment providers due to fears that buyers can falsely claim not to have received the products and claim a refund. As such, they demand higher prices for those who insist on using this service.[29]

The noted migration of online IWT away from e-commerce websites onto more private platforms may also suggest that the guaranteed transaction services offered by large companies are not playing a major role in IWT. However, as the case revealed by PEGAS demonstrates, smaller service providers have the potential to play an important role, particularly in the online live pet trade.

Direct deposits

Investigations into the online IWT suggest that traders sometimes prefer to use direct deposits, or electronic transfers, directly from one bank account to another, as these offer a greater degree of privacy and can be harder to detect than other payment systems.

How does it work?

Direct deposits can be processed in a number of ways. Many regions of the world have automated networks for batch-clearing transactions between banks (such as the Automated Clearing House [ACH] in the US), which coordinate between all the banks in a given region using a computer network. Customers wishing to make a direct deposit can also instruct their bank to directly connect with a receiving bank using a wire transfer. The burden of regulatory compliance falls on the financial institutions themselves, overseen by those who run the networks (e.g. the National Automated Clearinghouse Association runs the operating policies and rules for the ACH). Regulatory frameworks and capabilities vary from region to region.

Considering the speed and potential for relative privacy offered by direct deposits, it is plausible that they may be popular among more organized wildlife traders, particularly those engaged in high-value trade. This theory is supported to some extent by anecdotal details in reports on the IWT. For example, undercover reporters investigating a transnational network involved in smuggling chimpanzees from West Africa to the Middle East, Asia and elsewhere were instructed to make payments for a chimpanzee into a bank account in Conakry, Guinea, which

was owned by the ringleader's father.[30] This network was implicated in the sale of a large number of chimpanzees, which they advertised by video from their base in Ivory Coast.

The WJC has also discovered that Vietnamese traffickers selling online to Chinese buyers use Chinese bank accounts to receive funds, which it proposes is part of a money-laundering process. The WJC identified 17 such bank accounts, suggesting an operation of some scale.[31]

Although it is plausible that direct deposits play an important role in the online IWT, and there is some anecdotal evidence to support this, investigations often refer to any non-guaranteed payment as 'direct', making it hard to know exactly if direct deposits, e-wallets or another system is being used.

Card payment system

The card payment system, which is primarily run by the Visa and MasterCard networks, has traditionally been the dominant force in the online payment ecosystem, particularly in the West. Although the networks are losing ground to alternative payment systems, they are likely to maintain a large share of the market (as much as 46 per cent by 2019, according to UNCTAD).[32]

How does it work?

The card payment system is a network that connects the bank of an issuer of funds with the bank of a recipient. In this system, a consumer buying a product uses funds from their bank account (this is called the issuing bank), while the merchant selling the product receives funds into a merchant bank account (held by an 'acquiring bank'). The card payment networks sit between the issuing and the acquiring bank, and process all communications, ensuring ubiquity and allowing smooth payment. They also create and enforce the rules that maintain the integrity of the system and their own brand appeal.

Research has little to say directly about the role of the card payment networks in the online IWT. However, given their traditional dominance over online payments in the West, it is plausible that the Visa and MasterCard networks are used for transactions in these markets. In particular, customers buying from retailers may prefer to use a method they know and feel comfortable with. As an example from a comparable field, the card payment system is used extensively in the online sale of counterfeit goods in the West (more on this later in the report).

Market research into the buying habits of online customers in the IWT may help clarify the extent to which denying traders use of the card payment system would undermine their ability to reach markets in the West. For example, if a sizeable proportion of those buying illegal wildlife products online in Europe are opportunistic shoppers with minimal criminal intent – as suggested by one CITES official[33] – then a trader's unwillingness to accept payment through Visa or MasterCard could prove decisive in disrupting business in this market.

Cash on delivery, mobile money

Poorer markets with under-banked populations are less likely to adopt electronic payments. For example, a 2015 study found that 90 per cent of online transactions in Egypt are settled by cash on delivery.[34] In the West, cash on delivery is also popular as a means of payment for peer-to-peer sales on sites such as Craigslist.[35]

In a paper on illicit trade and organized crime in Europe, the Royal United Services Institute (RUSI) highlights the challenges posed to law enforcement in tracing financial flows where cash on delivery, which ensures anonymity to both seller and purchaser, is used.[36] If used in the online IWT, cash on delivery is unlikely to offer opportunities for monitoring or intervention.

Another payment system popular in under-banked populations is mobile money. This method, which is popular in sub-Saharan Africa, allows mobile users to deposit or withdraw money, or transfer credit on their mobile phones between service providers or individuals without the need for a bank account. Although the RUSI has noted the use of mobile money in the offline ivory trade in East Africa,[37] the World Bank cites a lack of evidence that mobile money is used for money laundering or other financial crimes in Africa.[38] This may be due to the limits on transaction sizes, and the relative ease of tracing users of the system.

Crypto currencies and the dark web

The dark web and crypto currencies have gained infamy for their role in the online drugs, arms and child-pornography markets, leading to questions about the potential exploitation of these tools by online wildlife traffickers. However, investigations have found little evidence of illicit wildlife trading taking place on the dark web, with most researchers presuming that the ease and low risk of trading on the surface web leave little incentive for illicit traders to seek shelter in darker recesses.[39] In light of this, some have cautioned journalists and activists against sting operations that might drive the online IWT underground, where the challenges facing law enforcement are so much greater.

Investigations have found little evidence of illicit wildlife trading taking place on the dark web.

Given the highly dynamic nature of crypto currencies, it is difficult to predict how it would play out if the IWT were to migrate into this area of the internet. Low-tech investigatory techniques have in the past proved effective at dismantling criminal networks hiding behind crypto currencies. For example, the identity of the founder of illicit dark-net drugs bazaar Silk Road, Ross Ulbricht, was, ironically, discovered by a tax investigator who collated fragments of his activities on the surface web.[40] On a more technical level, law enforcement and academic researchers are inventing new means of tackling the anonymity of Bitcoin and other crypto currencies through money-laundering techniques or resource-intensive analyses of blockchain that can reveal the identities of buyers and sellers.[41]

Given the key role played by crypto currencies across a wide range of illicit activities, it is likely that law enforcement will continue to focus on ways to better monitor and regulate their use by criminals.

Disrupting illicit trade by targeting online payment: The example of counterfeit goods

The fractured nature of e-payments and the lack of a clear typology or list of red flags for the online IWT means that committed traders have the advantage when it comes to avoiding detection through financial flows. However, the monitoring initiatives of groups such as TRAFFIC and the WJC have already proved to be effective at identifying online wildlife traders. Linking this information with payment service providers in order to have their services withdrawn may bolster the effectiveness of these initiatives.

Efforts to block the online sale of counterfeit goods, such as fashion brands, software and pharmaceuticals, by targeting the payment systems they rely on therefore make an interesting comparison.

Cyberspace has driven huge growth in the sale of counterfeit goods. One estimate put the total value of counterfeit and pirated goods sold online in 2010 at more than $200 billion.[42] While it is impossible to accurately track the total volume of this market, it is highly likely that the figures have grown since then.

The online counterfeit trade has several significant similarities to illicit trade in wildlife. In both cases, the development of e-commerce has enabled illegal traders to access far larger markets, while simultaneously reducing their exposure. The transnational nature of the online counterfeit trade also presents similar challenges to those posed by the IWT. As one EU report into the issue summarized, 'A website may be registered in one country, the bank account for payments in another, consignments are sent from yet another country – all of these elements can be easily coordinated by criminals that do not reside in any of these countries.'[43]

Cyberspace has driven huge growth in the sale of counterfeit goods.

The online counterfeit trade is also able to make use of the dynamism of the internet to evade regulations. In a development that mirrors the nature of online IWT, there has been a noted shift in some aspects of the counterfeit trade to social media, such as Instagram, Facebook or WeChat.[44] Interestingly, WeChat established a brand-protection platform in 2016, which has been proactive in confronting this challenge.[45] The platform has reportedly handled more than 17 000 complaints, with 7 000 WeChat accounts being shut down.[46]

Due to the huge losses incurred by counterfeit goods, the public safety concerns (posed by substandard medicines and other products), and the commercial and lobbying power of global brands, there has been a considerable mobilization of resources to meet this emerging challenge. At the same time, however, the limitations of traditional law enforcement have led to a recognition of the need to follow the money, in particular by targeting online payment methods.

Perhaps the most interesting initiative in this area is the cross-sector International AntiCounterfeiting Coalition's (IACC) RogueBlock programme.[47] Established in 2012, RogueBlock (initially known as the Payment Processor Portal) is a collaboration between the IACC and the payment industry. It provides rights-holders with a means to easily notify payment service providers with information about websites that are selling counterfeit goods, ultimately with the aim of having the services withdrawn. The payment service providers involved in the programme include MasterCard, Visa International, Visa Europe, PayPal, MoneyGram, American Express, Discover, PULSE, Diners Club and Western Union. To date, RogueBlock claims to have terminated 5 000 individual merchant accounts, affecting over 200 000 websites.[48] The process involves the following steps:

- Rights-holders (who monitor the internet for infringements of their legal property rights) file a formal claim via the portal.
- The IACC investigates using a trace message (a test purchase that reveals information about the merchant).
- There is coordination with the National Intellectual Property Rights Coordination Center to avoid conflict with any ongoing investigations.
- Checks are made to identify additional merchant accounts.
- Finally, action is taken by the payment service provider (or the acquiring bank that holds the merchant account) based on information from the investigation.[49]

To summarize, by demonstrating to a payment processor, such as a card network or PayPal, that a merchant account using their system is in breach of their own policies (by selling counterfeit goods), the rights-holder is able to use the payment processor as an enforcer. The process exploits the fact that merchants are bound by the policies of

the payment processors, regardless of jurisdiction, giving the rights-holder global reach to act against infringers, and thereby overcoming the complexity of traditional law-enforcement actors having to respond to a transnational crime.

The loss of a merchant account can spell significant disruption for counterfeit traders. Merchant accounts are time-consuming to set up – a process made more complex if acquiring banks have been pressured into not doing business with them due to repeated closures.[50]

In response to the IACC initiative, traders have adopted strategies to mitigate the damage done by losing a merchant account, which complicates the process for RogueBlock. These include:[51]

- Multiple merchant accounts – a trader sets up several accounts with the same acquiring bank, thereby spreading charge-backs (arising from complaints from consumers) and minimizing the effect of having one merchant account shut down.
- Multiple acquiring banks – the same as above, only the trader sets up merchant accounts at several acquiring banks.
- Aggregation – a common counterfeit tactic whereby a single merchant account holder acts as a front for multiple traders and several websites.

Other initiatives similar to RogueBlock exist to target more specific areas affected by the online counterfeit trade. For example, the Center for Safe Internet Pharmacies removes payment services from online pharmacies identified as selling counterfeit or fake medicine.[52]

Likewise, in the recording industry, the International Federation of the Phonographic Industry launched a programme in 2011 where it submits, on behalf of its members, evidence regarding unlicensed sites to the City of London Police to investigate.[53] If the site is found to be unlawful, the police pass on the details to payment service providers, who can then choose to cease working with the merchant account associated with the site. Participants in the programme include MasterCard, Visa, PayPal, PaySafeCard, American Express, Monitise, PhonePayPlus and Zong.

Similarly, a 2012 paper describes an effective intervention in the online trade of counterfeit software, primarily coordinated with card payment networks.[54]

Although these initiatives to respond to the online counterfeit trade provide a valuable precedent for the illicit online wildlife trade, it is clear that they only go so far in terms of their practical applicability to the IWT. Most obviously, RogueBlock relies on the participation of ubiquitous payment service providers, such as PayPal or the card networks, that are willing to cooperate in imposing their policies. There also needs to be an acquiring bank willing to close down the identified merchant account, and a means to make opening new merchant accounts onerous.

More generally, there appears to be considerable concentration in the operations of counterfeit traders, born of the need for efficiencies of scale. For example, the US Joint Strategic Plan on Intellectual Property Enforcement cites evidence that 90 per cent of accounts used to process credit-card payments on websites dedicated to the counterfeit trade are concentrated in three Chinese banks.[55] By contrast, the online IWT is fractured. As already discussed, it appears that different markets make use of different forms of payment depending on the region, the kind of products/animals being traded and the scale of the operation. As such, it seems unlikely that any of the payment service providers have a sufficiently dominating presence across online illicit wildlife trading marketplaces to have a major disruptive impact on the global trade if their activities were blocked.

Perhaps more seriously, it is not clear from current research to what extent illegal-wildlife traders rely on merchant accounts (held with acquiring banks, through aggregators, or directly with e-wallets such as PayPal and WeChat Pay), or if most simply use checking accounts that have limited payment options but are far easier to open than a merchant account – making the cost imposed by this kind of intervention less damaging.

In many cases, then, it may be ineffective to target the illicit trade in wildlife through payment service providers. Having said that, research has revealed areas where the online IWT is carried out through payment service providers with whom cooperation could be fruitful – the use of WeChat Pay in China is a key example.

The establishment of the Online Settlement Platform for Non-Bank Payment Institutions in China is particularly relevant in this light. This clearing house will bring together payment service providers and create a platform that shares transaction information. Hence, it may provide an opportunity for cooperation between all the major non-bank payment service providers in China and online monitoring programmes, such as the one developed by TRAFFIC, to deny wildlife traders access to payment services. Importantly, the clearing house is comprehensive, meaning that an effective campaign to shut down offending accounts would leave little room for traders to use other means to collect payment – at least in China.

Conclusion

Given the great variety of electronic payment methods and the fractured nature of the online IWT, there is unlikely to be a silver bullet in the form of a 'follow the money' approach to this global scourge. However, the fact remains that any significant trade carried out over the internet must rely on some kind of electronic payment. As regulators catch up with technological innovators, new opportunities to target illicit traders by monitoring the payment systems they rely on will most likely emerge. One potentially fruitful example of this, outlined above, is the Online Settlement Platform for Non-Bank Payment Institutions in China. Similar initiatives are likely to follow, particularly in Asian countries, where innovation in this field is most concentrated. As such, developments in FinTech regulatory regimes should be monitored for emerging opportunities to target payment systems.

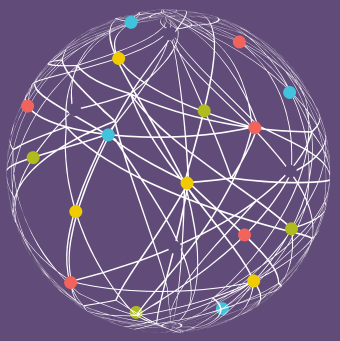
Environmental campaign groups have already developed the kind of online monitoring capabilities that would provide the intelligence vital for a sustained campaign to deny illegal wildlife traders access to payment systems. However, detailed information on identified traders' financial arrangements tends to be lacking, and gathering this information is complex, both ethically and logistically.[56] While there may not be the resources to undertake such a task across the global online IWT, further research may identify distinct markets where the ingredients for an effective intervention of this kind exist.

Given the great variety of electronic payment methods and the fractured nature of the online IWT, there is unlikely to be a silver bullet in the form of a 'follow the money' approach to this global scourge.

Notes

1. London Conference on the Illegal Wildlife Trade, Declaration, 12–13 February 2014, https://cites.org/sites/default/files/eng/news/sundry/2014/london-wildlife-conference-declaration-140213.pdf.
2. Hanoi Conference on Illegal Wildlife Trade, Statement, 17–18 November 2016, http://iwthanoi.vn/wpcontent/themes/cites/template/statement/Hanoi%20Statement%20on%20Illegal%20Wildlife%20Trade%20(English).pdf.
3. Matt Lowton, Anti-corruption tools exist – now they must be used to help fight illegal wildlife trade, Environmental Investigation Agency, 8 December 2017, https://eia-international.org/anti-corruption-tools-exist-now-must-used-help-fight-illegal-wildlife-trade.
4. Environmental Investigations Agency, Japan's illegal ivory trade and fraudulent registration of ivory tusks, 2015, https://content.eia-global.org/posts/documents/000/000/316/original/EIA_Japans_Illegal_Ivory_Trade_12102015.pdf?1468248072.
5. International Fund for Animal Welfare, Wanted – dead or alive: Exposing online wildlife trade, https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/IFAW-Wanted-Dead-or-Alive-Exposing-Online-Wildlife-Trade-2014.pdf.
6. Interpol Environmental Crime Programme, Project Web: An investigation into the ivory trade over the internet within the European Union, February 2013, https://s3.amazonaws.com/ifaw-pantheon/sites/default/files/legacy/Project%20Web%20-%20PUBLIC.pdf.
7. Guan Jing, Xu Ling, Deadly messaging: Illegal ivory trade in China's social media, TRAFFIC, November 2015, http://www.traffic.org/publication/15_Deadly_Messaging_Illegal_Ivory_Trade_in_China.pdf.
8. Convention on International Trade in Endangered Species of Wild Fauna and Flora, Decisions of the Conference of the Parties to CITES in effect after its 17th meeting, 15.57 & 17.92 - 17.96, CITES, 2016.
9. International Fund for Animal Welfare, E-commerce and wildlife cybercrime: Effective policies and practices to stem the growth of illicit trade, OECD High Level Risk Forum, 28–29 March 2017.
10. See, for example, Elizabeth Davis, Tech industry leaders join forces against online wildlife trafficking, World Wildlife Fund, Washington DC, 12 August 2016, https://www.worldwildlife.org/press-releases/tech-industry-leaders-join-forces-against-online-wildlife-trafficking.
11. Kanitha Krishnasamy and Sarah Stoner, Trading faces: A rapid assessment on the use of Facebook to trade wildlife in peninsular Malaysia, TRAFFIC, Selangor, Malaysia, March 2016, http://www.traffic.org/publication/16_Trading_Faces.pdf. See also Liu Caiyu, Chinese internet firms to share intelligence with govt on illegal wildlife trade, *Global Times*, 22 November 2017, http://www.globaltimes.cn/content/1076672.shtml.
12. Tatiana Tropina, Do digital technologies facilitate illicit financial flows?, World Bank, 2016, http://pubdocs.worldbank.org/en/396751453906608518/WDR16-BP-Do-Digital-Technologies-Facilitate-Illicit-Financial-Flows-Tropina.pdf.
13. Xiao Yu and Wang Jia, Moving targets: Tracking online sales of illegal wildlife products in China, TRAFFIC, February 2015, http://static1.1.sqspcdn.com/static/f/157301/26245505/1432122394320/China-monitoring-report.pdf.
14. UNCTAD, Information economy report 2017: Digitalization, trade and development, 23 October 2017, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.
15. Emailed correspondence with industry analyst, 16 March 2017.
16. Rahimi Yunis, E-wallet platforms to create 'tsunami' of cashless payment this year, *The Malaysian Reserve*, 23 January 2018, https://themalaysianreserve.com/2018/01/23/e-wallet-platforms-create-tsunami-cashless-payment-year/.
17. Tatiana Tropina, Do digital technologies facilitate illicit financial flows?, World Bank, 2016, http://pubdocs.worldbank.org/en/396751453906608518/WDR16-BP-Do-Digital-Technologies-Facilitate-Illicit-Financial-Flows-Tropina.pdf.
18. Gabriel Wildau, China targets mobile payment oligopoly with clearing mandate, *Financial Times*, 9 August 2017, https://www.ft.com/content/3bcb5150-7cce-11e7-9108-edda0bcbc928.
19. Guan Jing, Xu Ling, Deadly messaging: Illegal ivory trade in China's social media, TRAFFIC, November 2015, http://www.traffic.org/publication/15_Deadly_Messaging_Illegal_Ivory_Trade_in_China.pdf.
20. Ibid.
21. Wildlife Justice Commission, Operation Phoenix, December 2017, https://wildlifejustice.org/wp-content/uploads/2018/01/Phoenix-Briefing-Public.pdf.
22. Project to End Great Ape Slavery, PEGAS hosts illegal wildlife trade cyber-crime Workshop, 21 April 2017, https://freetheapes.org/2017/04/21/pegas-hosts-illegal-wildlife-trade-cyber-crime-workshop-2/.
23. Gabriel Wildau, China targets mobile payment oligopoly with clearing mandate, *Financial Times*, 9 August 2017, https://www.ft.com/content/3bcb5150-7cce-11e7-9108-edda0bcbc928.
24. Timmy Shen, WeChat Pay now allows users to bind overseas credit cards, TechNode, 24 January 2018, https://technode.com/2018/01/24/wechat-pay-now-allows-users-to-bind-overseas-credit-cards/.
25. Xiao Yu and Wang Jia, Moving targets: Tracking online sales of illegal wildlife products in China, TRAFFIC, February 2015, http://static1.1.sqspcdn.com/static/f/157301/26245505/1432122394320/China-monitoring-report.pdf.
26. Lerong Lu, How a little ant challenges giant banks? The rise of Ant Financial (Alipay)'s fintech empire and relevant regulatory concerns, *International Company and Commercial Law Review*, 28, 1, 12–30.
27. UNCTAD, Information economy report 2017: Digitalization, trade and development, 23 October 2017, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.
28. Project to End Great Ape Slavery, Indonesian traffickers' transaction method of selling illegal wildlife: Rekber, PEGAS, 14 May 2018, https://freetheapes.org/2018/05/14/indonesian-traffickers-transaction-method-of-selling-illegal-wildlife-rekber/.
29. Guan Jing and Xu Ling, Deadly messaging: Illegal ivory trade in China's social media, TRAFFIC, November 2015, http://www.traffic.org/publication/15_Deadly_Messaging_Illegal_Ivory_Trade_in_China.pdf.
30. David Shukman and Sam Piranty, The secret trade in baby chimps, BBC News, 30 January 2017, http://www.bbc.co.uk/news/resources/idt-5e8c4bac-c236-4cd9-bacc-db96d733f6cf.

31. Wildlife Justice Commission, Operation Phoenix, December 2017, https://wildlifejustice.org/wp-content/uploads/2018/01/Phoenix-Briefing-Public.pdf.
32. UNCTAD, Information economy report 2017: Digitalization, trade and development, UNCTAD, 23 October 2017, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.
33. Skype interview with CITES official, 24 May 2018. We also note, for example, the case of a UK man found guilty of selling rare animal parts on eBay, profiting by as much as £20 000 a month. He was found to be misleading his customers about the legality of his products. See Taxidermist sold pickled lizards and monkey heads on eBay, BBC News, 17 January 2017, http://www.bbc.com/news/uk-england-devon-38658166.
34. UNCTAD, Information economy report 2017: Digitalization, trade and development, 23 October 2017, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.
35. Craigslist recommends that customers should deal only with people they have met in person; see https://www.craigslist.org/about/scams.
36. Clare Ellis, On tap Europe: Organised crime and illicit trade in tobacco, alcohol and pharmaceuticals, Royal United Services Institute for Defence and Security Studies, 17 March 2012, https://rusi.org/sites/default/files/201703_rusi_whr_217_on_tap_europe_updated_low-res.pdf.
37. Cathy Haenlein and Tom Keatinge, Follow the money: Using financial investigation to combat wildlife crime, Royal United Services Institute for Defence and Security Studies, September 2017, https://rusi.org/sites/default/files/201709_rusi_follow_the_money_haenlein.keatinge.pdf.
38. Tatiana Tropina, Do digital technologies facilitate illicit financial flows?, World Bank, 2016, http://pubdocs.worldbank.org/en/396751453906608518/WDR16-BP-Do-Digital-Technologies-Facilitate-Illicit-Financial-Flows-Tropina.pdf.
39. David L Roberts and Julio Hernandez-Castro, Bycatch and illegal wildlife trade on the dark web, *Oryx*, 51, 3, 393–394.
40. Nathaniel Popper, The tax sleuth who took down a drug lord, *The New York Times*, 25 December 2015.
41. Kristy Kruithof et al, Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands, Rand Europe, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1607/RAND_RR1607.pdf.
42. Business Action to Stop Counterfeiting and Piracy, International Chamber of Commerce, Roles and responsibilities of intermediaries: Fighting counterfeiting and piracy in the supply chain, March 2015, https://cdn.iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf.
43. European Union Intellectual Property Office, 2017 Situation report on counterfeiting and piracy in the European Union, https://buysaferx.pharmacy//wp-content/uploads/2018/03/counterfeiting_and_piracy_in_the_european_union.pdf.
44. Paul Mandell, They're not faking it: China needs cooperation to combat counterfeiting, Trademarks & Brands Online, 1 June 2016, https://www.trademarksandbrandsonline.com/article/they-re-not-faking-it-china-needs-cooperation-to-combat-counterfeiting; Roxanne Elings, New trends in online counterfeiting require updated enforcement policies, *World Trademark Review*, 7 February 2017, http://www.worldtrademarkreview.com/Intelligence/Online-Brand-Enforcement/2017/Chapters/New-trends-in-online-counterfeiting-require-updated-enforcement-policies.
45. PR Newswire, WeChat tightens crackdown against counterfeit with major improvements, Guangzhou, China, 13 March 2018, https://www.prnewswire.com/news-releases/wechat-tightens-crackdown-against-counterfeit-with-major-improvements-300613212.html.
46. Zhang Zhao, WeChat committed to active copyright protection, *China Daily*, 20 January 2016, http://www.chinadaily.com.cn/kindle/2016-01/20/content_23165536.htm.
47. See IACC website, https://www.iacc.org/online-initiatives/rogueblock.
48. Ibid.
49. Business Action to Stop Counterfeiting and Piracy, International Chamber of Commerce, Roles and responsibilities of intermediaries: Fighting counterfeiting and piracy in the supply chain, March 2015, https://cdn.iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf.
50. Damon McCoy et al, Priceless: The role of payments in abuse-advertised goods, 19th ACM Conference on Computer and Communications Security, Raleigh, North Carolina, 16–18 October 2012, https://cseweb.ucsd.edu/~savage/papers/CCS12Priceless.pdf.
51. The following is taken from Kristina Montanaro, IACC Payment Processor Portal Program: First year statistical review, IACC, October 2012, http://docplayer.net/2433238-International-anticounterfeiting-coalition-iacc-payment-processor-portal-program-first-year-statistical-review.html.
52. Business Action to Stop Counterfeiting and Piracy, International Chamber of Commerce, Roles and responsibilities of intermediaries: Fighting counterfeiting and piracy in the supply chain, March 2015, https://cdn.iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf.
53. Ibid.
54. Damon McCoy et al, Priceless: The role of payments in abuse-advertised goods, 19th ACM Conference on Computer and Communications Security, Raleigh, North Carolina, 16–18 October 2012, https://cseweb.ucsd.edu/~savage/papers/CCS12Priceless.pdf.
55. US Joint Strategic Plan on Intellectual Property Enforcement, Supporting innovation, creativity & enterprise: Charting a path ahead, FY 2017–2019, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/2016jointstrategicplan.pdf.
56. Using trace messages to uncover bank account information is ethically complex, especially in the IWT, due to the risk that they stimulate the market. It is logistically complex due to the need to source appropriate payment methods (e.g. a credit card or an e-wallet account) that can be used to make the payment – a sustained campaign requires a large number of such methods to avoid detection by the traders. RogueBlock and the other initiatives mentioned above have grappled with the same issues and developed responses, such as partnering with payment card issuers (to secure a reliable source of cards); and using pre-paid cards with insufficient balance to prevent the payments from being completed. For a useful summary of these issues and responses, see Kristina Montanaro, IACC Payment Processor Portal Program: First year statistical review, IACC, October 2012, p 20, http://docplayer.net/2433238-International-anticounterfeiting-coalition-iacc-payment-processor-portal-program-first-year-statistical-review.html.



THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

www.globalinitiative.net

A NETWORK TO COUNTER NETWORKS