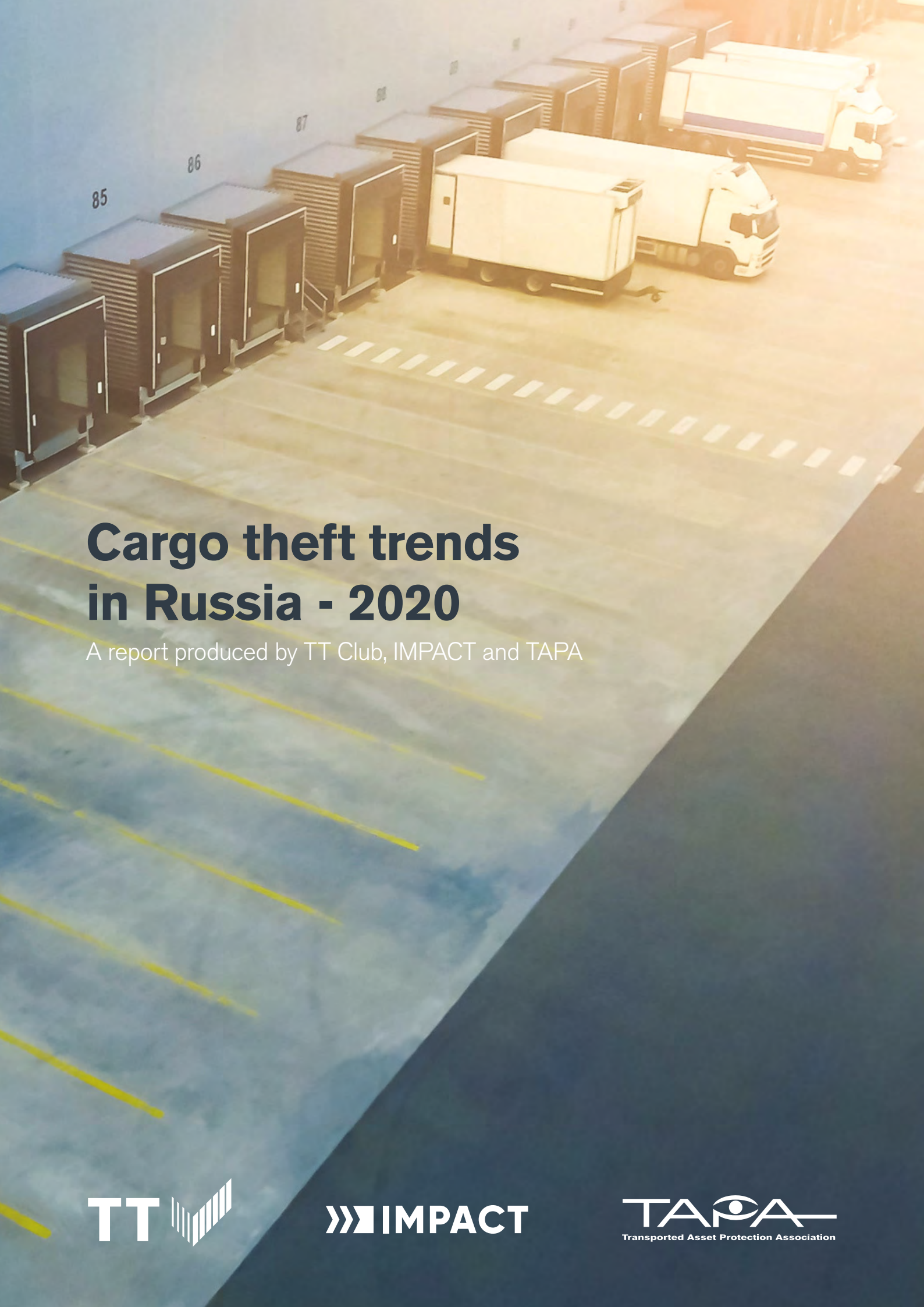


Cargo theft trends in Russia - 2020

A report produced by TT Club, IMPACT and TAPA

TT

IMPACT

TAPA
Transported Asset Protection Association

Contents

Introduction p05

Threat overview p08 & p09

Modus operandi p10

Most targeted cargo p12

Focus on specific commodities p14

A focus on fraud p22

Loss prevention guidance p25

IMPACT is a partnership initiative for information exchange and industry collaboration to minimize risks in the supply chain and reduce cargo losses in Russia.

Industry's first innovative digital platform for collecting and analysing intelligence on cargo theft, providing online vetting services to identify individuals, forwarding and transport entities, and vehicles that routinely take part in fraudulent pickup and full truck loss incidents.

IMPACT was established in 2019 by leading experts in supply chain and corporate security with a vision to establish open collaboration within the industry for legitimate data exchange on cargo theft threats in Russia, as well as share intelligence and best practices with leading international institutions and companies who are active in security risk management, fraud prevention and cargo protection to enable effective incident data exchange, improve security awareness and theft prevention, referencing various consulting services and solutions.

TT Club is the established market-leading independent provider of mutual insurance and related risk management services to the international transport and logistics industry. The Club's services include specialist underwriting, claims management and risk and loss management advice, supported by a global office network. TT Club's primary objective is to help make the industry safer and more secure. Established in 1968, TT Club has more than 1100 Members, spanning owners and operators, ports and terminals, and logistics companies, working across maritime, road, rail, and air. Members range from some of the world's largest logistics operators to smaller, bespoke companies managing similar risks. The Club is renowned for its high-quality service, in-depth industry knowledge and enduring Member loyalty. It retains more than 93% of its Members with a third of its entire membership having chosen to insure with the Club for 20 years or more.

TT Club is managed by Thomas Miller - an independent and international provider of insurance, professional and investment services.

The Transported Asset Protection Association (TAPA) is a not-for-profit industry Association founded in 1997 to help Manufacturers/Shippers and their Logistics Service Providers minimise losses from their supply chains resulting from cargo thefts. Today, the Association provides a host of industry standards, training, incident intelligence, route planning and networking tools and opportunities which are used by its member companies as part of their own in-house supply chain security programmes to mitigate risk and optimise loss prevention. Its membership also includes Insurers, Security Service Providers and Law Enforcement Agencies.

For more information, go to www.tapa-global.org

Introduction

Industry data suggests that the road freight market in Russia grew by almost 10% in 2020, despite the effects of the spring lockdown in April-May. 2020 witnessed a notable growth in transportation in Russia in almost all major directions. Transportation from the Moscow region specifically gained momentum, illustrating that the Central region continues to grow as a freight hub.

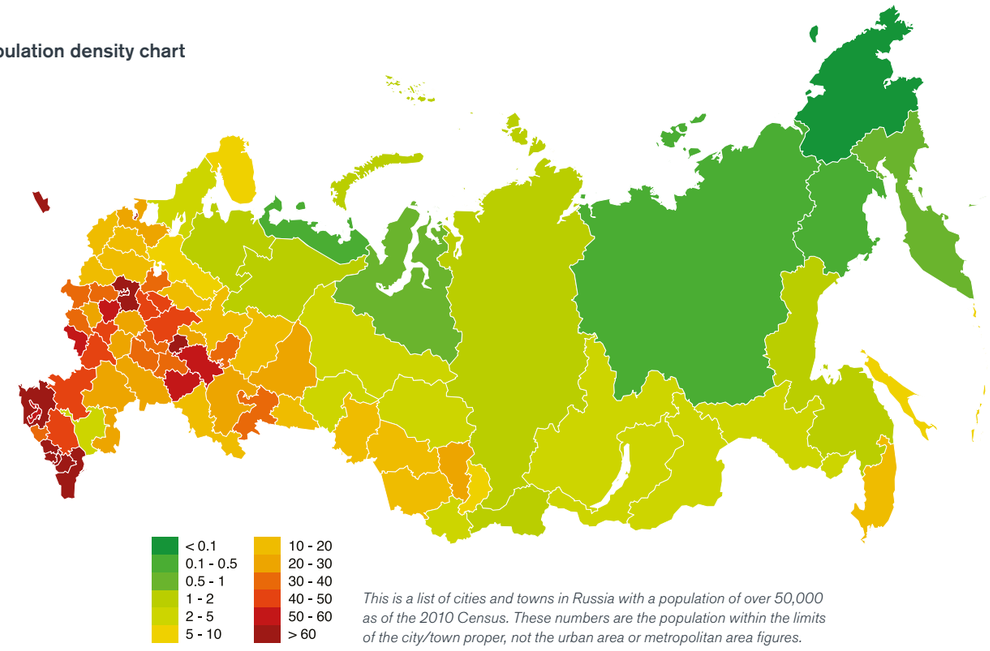
Cargo theft in Russia has become a lucrative industry, running into 100's millions of dollars, plaguing local supply chains, disrupting local and international business. Cargo theft incidents range from small-scale pilferage and curtain slashing, while vehicles are parked at unsecured parking areas, to full-truckload theft and warehouse burglaries.

Organised criminal networks continuously seek ways to evade security controls to access, transport, and realise funds from legitimate goods on the grey market. All categories of goods are at risk of theft particularly during road haulage. The modus operandi used to carry out theft are striking in their diversity, however most cargo thefts are facilitated through complicated multi-stage fraud schemes involving fake carriers, smart front drivers and forged registration of vehicles. The insider threat is also high, where logistics managers are able to create accounts for logistics companies on various internet freight exchanges.

Geographical and economic background

Russia, the largest country in the world in terms of land area, is administratively divided into 8 major areas, known as federal districts. The districts vary in size, population density, level of infrastructure, industrial activity, and related socio-economic dynamics such as consumption and associated criminal activities. The most populated districts are located in the Western part of the country housing more than 83% of the total population. Federal districts are comprised of smaller administrative units called regions (Oblast - in Russian) .

Population density chart



This is a list of cities and towns in Russia with a population of over 50,000 as of the 2010 Census. These numbers are the population within the limits of the city/town proper, not the urban area or metropolitan area figures.

Central, Volga, South (including North Caucasus), North-west and Urals federal districts are the most industrially developed areas with major production facilities, storage and warehousing facilities as well as logistics and transport operations supporting them. Unequal distribution of industrial and logistics activities as well as consumption is driven by the development dynamics of the district. Moscow region outperforms all other regional centres in gross regional product (GRP) and consumption per capita and accounts for around 55% of Russia's overall warehouse capacity. These factors drive most of trends in logistics and transportation sectors, as well as associated criminal trends.

Data sources

Cargo theft in Russia is heavily under-reported as in many other parts of the CIS area and Europe. As the leading independent data source in Russia, IMPACT created an analytical tool that collects all available data from any open source to highlight the magnitude of the problem, developing a resource that members can benefit from and conduct meaningful risk assessment for their supply chains in Russia and CIS region.

The data in this report is a combination of IMPACT data sourced from its partners, open-source media, publicly available arbitrary court proceedings related to the loss of cargo, and TT Club claim data for the periods 2019 and 2020. Both IMPACT and TT Club acknowledge that the incident information represents only a part of the real number of cargo crime in Russia as large numbers of incidents are suspected to be unreported to either the Police or insurers. However, combined statistical volume of more than 300 cases in 2020 (500 in 2019) represent a sufficient volume of data and provides an opportunity to apply analytical methods and ultimately identify current and emerging criminal trends in the local cargo transportation sector.

In preparation of this report, IMPACT and TT Club made analysis of official cargo theft statistics available in Russia for a 5-year period (2016-2020) concluding that Russia observes a general downward trend of cargo crime. According to the official data, the total number of cargo-related incidents in Russia dropped 45% from 2452 cases in 2016 to 1334 in 2020. The level of violent attacks also has a gradual reduction trend with 370 incidents registered in 2016 down to 235 in 2020.

Incident overview

The COVID-19 pandemic that took hold through 2020 impacted historical cargo theft trends in a multitude of ways. Local and national restrictions on general movement affected the thieves' ability to move undetected undertaking their activities, influencing how they operated. The economic impact of the pandemic influenced market forces and therefore the cargoes primarily targeted by criminals. The overall number of recorded incidents reduced 2019 to 2020 by approximately 35%. This being a culmination of the above factors and the fact those general volumes were lower during 2020. The value of the average loss through 2020 reduced to US$38,807.00 from US$42,972.00 in 2019.

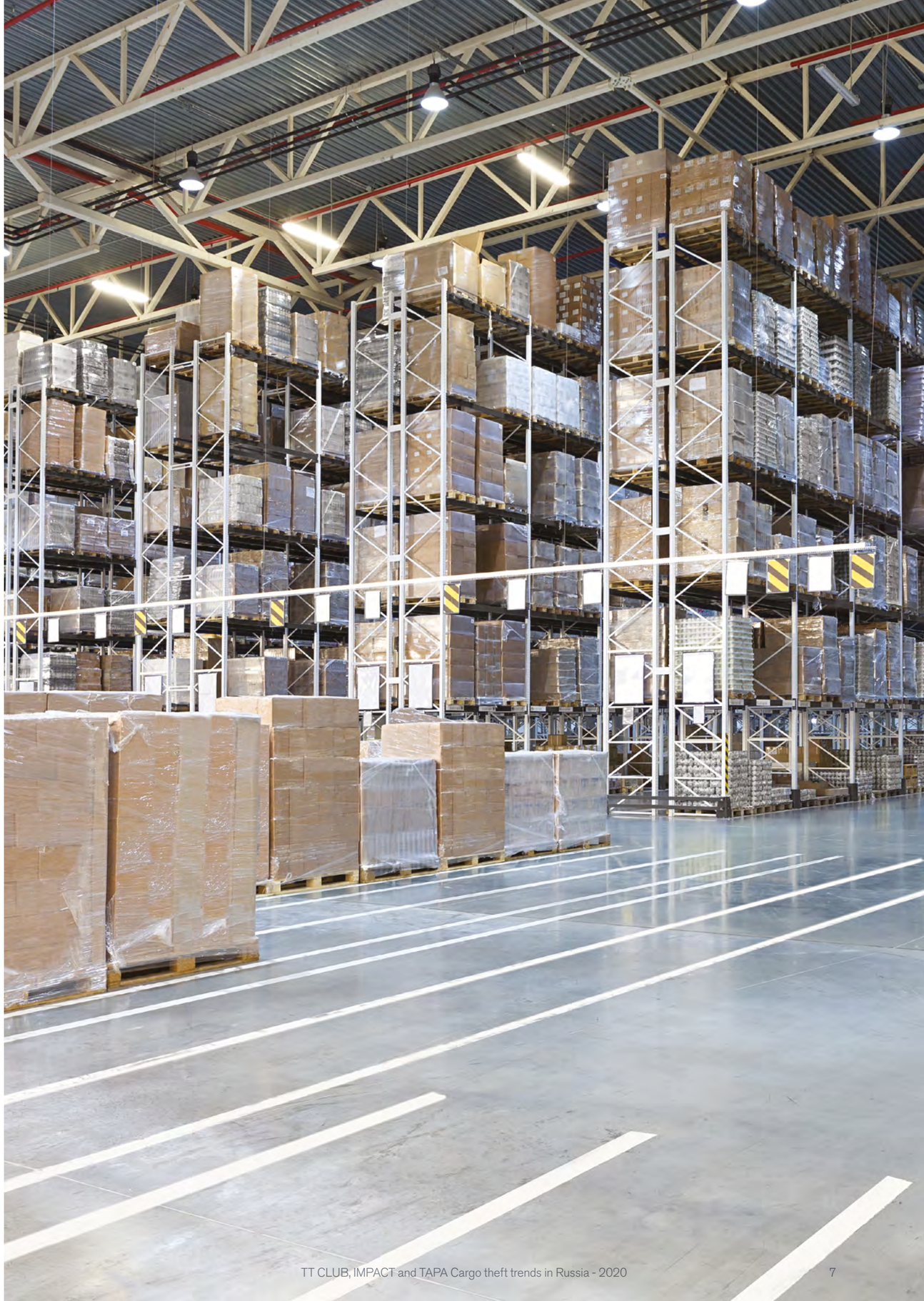
Need for action

In developing this report, IMPACT, TT Club and TAPA recognise that there is a need to increase risk awareness and promote efficient preventative security processes. Providing meaningful cargo crime data and analysis thereof will empower the logistics and manufacturing industries operating in Russia to improve understanding of the risks and mitigate their exposure.

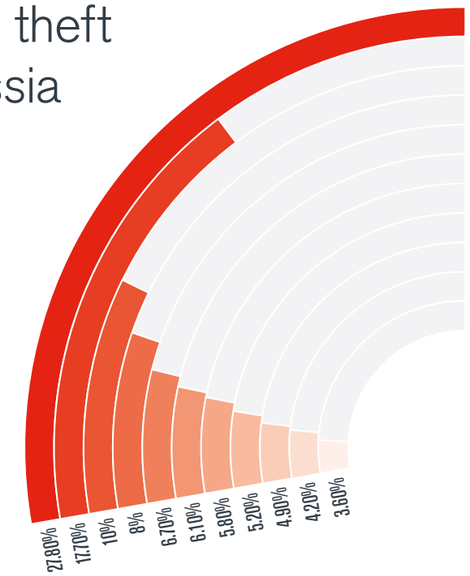
It would be prudent for all involved in the supply chain, from manufacturers through to road haulage businesses, to develop an awareness of the risks highlighted in this report. Thereafter procedures and training can be developed to assist mitigating these types of loss.

According to official data cargo-related incidents in Russia dropped 45% from 2016 to 2020

↓45%



Cargo theft in Russia 2020



- **Food & Beverage**
- **Other** *includes 11 categories (Sporting goods, pharma & tobacco)
- **Metal**
- **Household appliances**
- **Auto parts**
- **Household goods**
- **Construction materials**
- **Clothes, shoes & textiles**
- **Chemicals**
- **Industrial equipment**
- **Alcohol**

83.2% of thefts involve fraudulent activity

83.2%

↓12.2%

↓40.8%

↑25%

↓48%

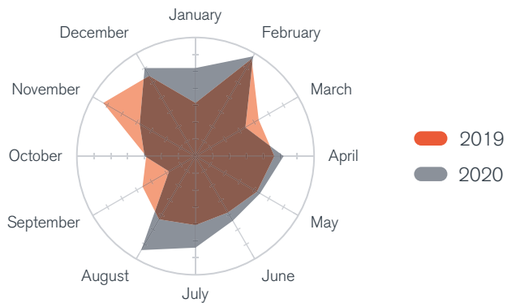
↓51.9%

↓38.5%

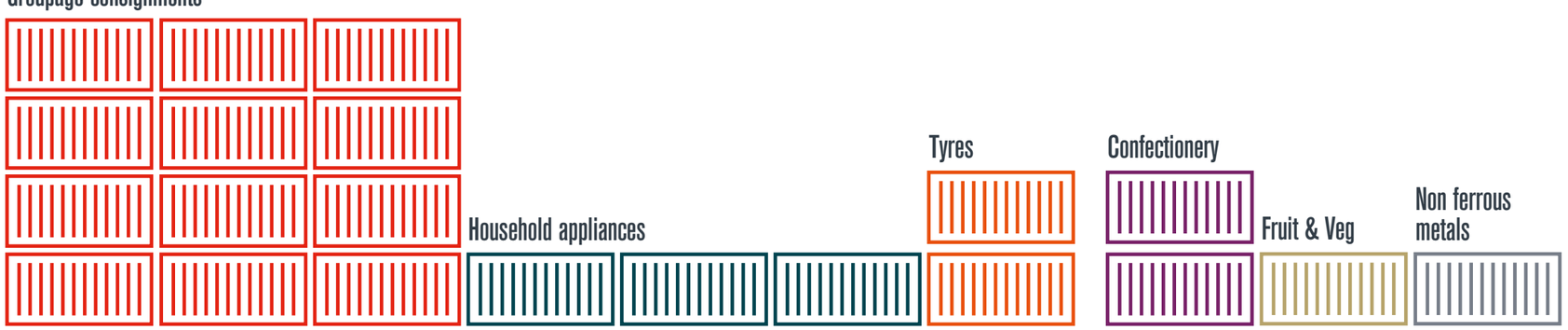
↓25%

↑100%
* year 1 = 0

Theft by month



Groupage consignments



Average value

↓9.69%

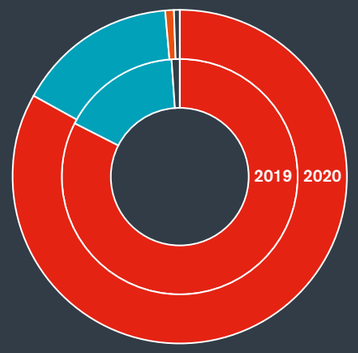
2019 3,177,992₽
42,972$

2020 2,768,332₽
38,807$

The data in this report is a combination of IMPACT data and TT Club claim data for the periods 2019 and 2020.

Modus operandi

The way that thieves infiltrate the supply chain remained stable from 2019 running through 2020. The primary modus operandi being various fraudulent methods and theft from parked trucks. There has been a slight upward trend in fraudulent activity through 2020, accounting for over 83% of reported incidents by frequency. A partial explanation being the impact influence that the periods of COVID-19 lockdown through 2020 preventing free movement of the thieves to target parked trucks.

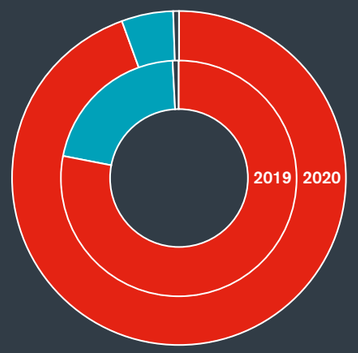


	2019		2020
Fraud	82.7%	↑	83.2%
Theft	16.3%	↓	15.6%
Robbery	N/A	↑	0.9%
Other	1.0%	↓	0.3%

By generating a complex chain of sub-contractors, bad actors create smoke screens behind which their activities can be hidden. The commonality of all of the fraudulent schemes is the person arriving at the loading place, which may be known to be part of the fraudsters' intentions or be used blindly. In both cases, the integrity of the driver during background checks is beyond doubt as all forms of identification and vehicle documents will often be genuine. Only after the driver has collected the cargo do the criminals step in and, purporting to be the owner of the goods, redirect the truck and cargo to another destination. The driver has the potential to present risk, while they might appear themselves to be victims of the fraud, on occasion the driver is complicit to the theft, willingly violating rules to get paid for their services by any means.

Types of fraud

When we consider specifically the types of fraud that thieves employ, 2020 witnessed a significant shift away from forged documents that accounted for over 20% of incidents in 2019. Forged documents accounted for just 5% of incidents in 2020 resulting in a sharp increase in fraud thefts achieved through accessing cargo under seemingly legitimate auspices and then unloading the cargo at an unspecified location during carriage. According to independent research, cargo thefts in Russia annually account for losses of more than 15 billion Rubles. The main method of theft is fraud using falsified documents and redirecting drivers in transit by phone for unloading at a place not specified in the transport documents. The latter scheme, which from a legal perspective is challenging to build evidence to identify the criminal party, has become widespread in Russia.



	2019		2020
Unloaded at unspecified place	78.3%	↑	94.5%
Forged documents	20.9%	↓	5.1%
Other	0.8%	↓	0.4%

Criminals actively employ their risk-benefit analysis models to justify the specific way of attacking cargo. They realise that security controls in high-value sectors, such as tobacco are much stricter, resulting in a high risk of physical engagement with a security guard or Police who could intervene, preventing a theft. Therefore, to attempt theft of this type of cargo criminals need to invest significant resources like hiring (or buying) the truck, forging driver's ID, acquiring identity of a legitimate forwarder or carrier. For lower value cargo, organised criminals typically choose less resource and time consuming techniques that could involve the registration of a forwarder profile in a freight exchange and employing a driver who would agree to follow the criminals' instructions to unload goods in an unauthorised location, contrary to that specified in the shipping paperwork.

Recognising that thieves become ever more sophisticated in terms of ability to forge documents to access cargo, this activity is time intensive through the preparation stages and is not without risk. The shift witnessed in 2020 suggests that there are greater efficiencies employing alternative methods.

Driver's call diverting

How it works in practice…

This tactic is primarily used in single fraud attacks and often involves drivers who are unwittingly employed by fraudsters. According to our analysis this method is most popular amongst criminals because it is least resource-intensive and requires very little to organize the fraud. Usually, victims of this scheme are small and medium-size producers of food and multiple forwarding companies whose business model relies on small agent fees through the placement of orders on freight exchange platforms. Both categories of business have little or no baseline security checks against their subcontractors, which is the main attraction for criminals.

Actors: Typically, the actors in such schemes are:

1. **Shipper** - *manufacturer or goods owner who seek transportation services;*
2. **Freight forwarder** - *a legitimate logistic business providing services to the shipper;*
3. **Carrier** - *fraudulent entity, a business selected to perform the actual transportation on behalf of the forwarder;*
4. **Driver** - *an individual who is found on the market by the carrier to collect the goods from the shippers' premises.*

Step 1: Preparation and research

The fraudster presents itself as a legal entity that will play the role of the carrier company utilizing an account on the freight exchange. By an active search in the new freight orders and available vehicles, the fraudster identifies a potential driver and cargo that could match each other. Then the fraudster separately contacts the freight forwarder who placed the order and the driver who awaits a suitable load and by deceit obtains the necessary documents from both parties. The criminals then make an attractive offer to the driver (for example, payment in cash at unloading) with just one simple requirement – strictly follow their instructions.

The driver's identification is then presented to the forwarder who in turn sends them to the shipper to prepare all the shipment paperwork, including the power of attorney for the driver issued by the shipper to enable cargo pick up. At this stage, the fraudster replaces the driver's phone number with his own. The forwarder is now speaking with the criminals thinking they are talking to the driver. The real driver, feeling lucky to get a good job, awaits instruction from the fraudsters. Everything is ready to launch an attack.

Step 2: Loading, driver's call diverting

The driver arrives at the warehouse to pick up the goods. As the shipper and forwarder's offices are in different locations, nobody physically sees or verifies the paperwork or identification of the driver produced at the warehouse. Fraudsters continue to maintain communications with all the actors. The forwarding company and the shipper are convinced that they are speaking to the driver when giving him instructions for transportation, timings and unloading at destination. The driver however only maintains communication with the fraudsters. The loaded truck leaves the premises of the shipper.

Shortly after that, the fraudster calls the driver and diverts the truck to a nearby location, not specified in the transport documents. For the driver this scenario is attractive, as he does not need to drive too far, while receiving the fee for the performed service. Finally, the truck is unloaded to third party storage or another vehicle.

Step 3: Delaying alert and ceasing communication

For the shipper and the forwarder, the fraudster continues communication as if the driver has continued the journey. Calls are accepted for another day or two, building the illusion that the trip is in progress. However, when a delay in delivery becomes apparent there might be notification of a truck break down or unplanned repairs. This strategy is employed to delay an alarm and increase the time to perform similar attacks on other cargo of different shippers. When the criminals' objectives are achieved, the communication drops and enquiries start on the part of both – shipper and forwarder. Unfortunately, by this time, the goods are usually sold and the chances to recover cargo are minimal.

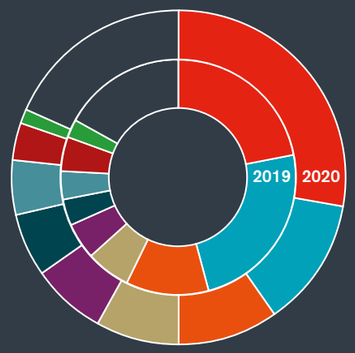
"I follow the instructions of those who pay me in cash!"

Most targeted cargo

IMPACT and TT Club data noted continuity in the two primary targeted cargo groupings in 2019 through 2020. Food and beverage cargoes remained the single most targeted, increasing from 22.1% to 27.8% in 2020 overall. This likely a result of market forces swinging in favour of necessity rather than luxury goods as an impact of the global pandemic.

As illustrated in the following analysis, the changing market forces during the COVID-19 pandemic influenced thieves targeting more essential cargo groups, witnessing a reduction in the frequency thefts of many other cargo groups. There are commonalities in seasonal variation when we look at 2019 versus 2020 data, February, August, November and December all witness spikes in activity. These seasonal variations can be commodity specific, in line with peaks in activity, for instance in the building trade. Geographical spread of incidents is influenced by a number of factors including population density and the primary industries active in the district.

Types of cargo theft



	2019		2020
Food & beverage	22.1%	↑	27.8%
Metal & cable	24.0%	↓	12.5%
Construction materials & Industrial equipment	11.3%	↓	9.8%
Household appliances & electronics	6.3%	↑	8.0%
Auto parts & tires	4.8%	↑	7.3%
Household goods	3.8%	↑	6.1%
Clothes, shoes & textiles	3.8%	↑	5.2%
Alcohol	4.8%	↓	3.6%
Chemicals	2.5%	↓	1.5%
Others *Includes 9 categories (Tobacco, Pharma, Sporting goods)	16.6%	↑	18.2%

Metals and cable products were the second most frequently targeted cargo group in both 2019 at 24%, reducing to 12.5% in 2020. Fundamental changes in the economic conditions and consumption market forces influenced which cargo groups were targeted through 2020. Generally, luxury goods was less theft attractive, influenced by what the ultimate buyer demands at a given time. Nevertheless, high-value cargo were still targeted in 2020, but with a slightly reduced frequency.

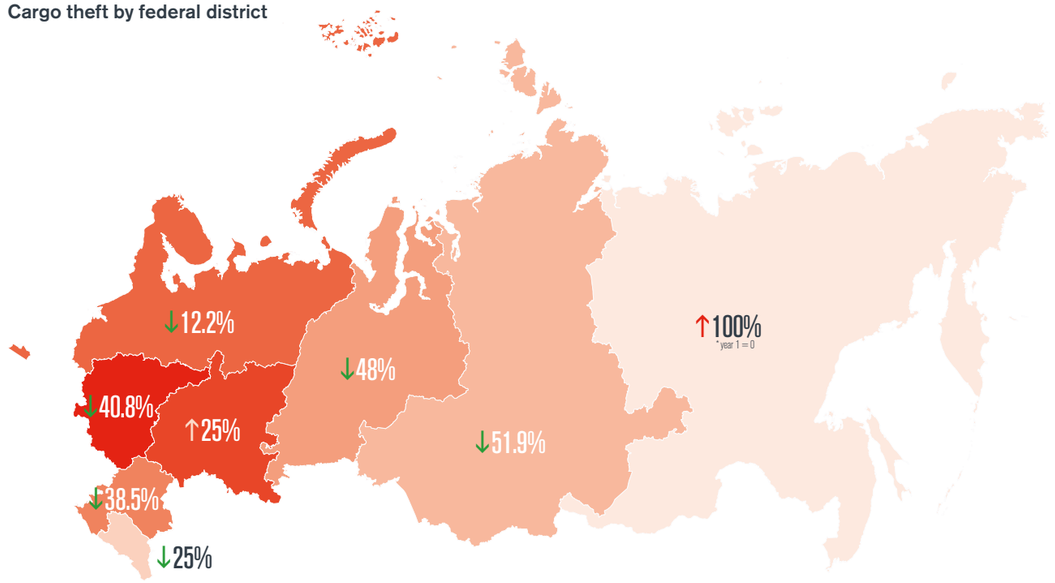
Construction materials and alcohol were two notable reductions through the period. Essential cargo groups such as household goods and appliances, clothes, shoes and textiles and to a lesser extent auto parts all witnessed an increase in frequency of theft in 2020.

At a granular level, confectionery, non-ferrous metals and groupage consignments remain in the top six most targeted commodities. In 2019 and 2020 groupage, consignments were by far the most targeted shipments. This in part influenced by the availability to access these shipments from distribution centres and the trend to fraudulently access cargo from such locations. Distribution centres naturally store a range of individual commodities, distributing into the hinterland a mixture on any given truck.

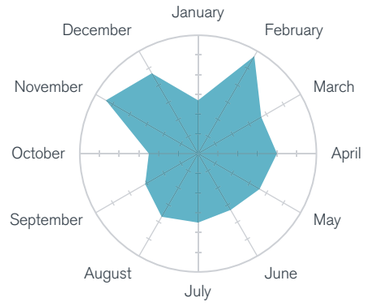
Electronic freight exchange

When considering electronic freight exchange services there are clearly many benefits. The intentions are commendable in reducing empty running miles and opening a large volume of available haulage capacity to those who use the service. While users benefit from greater efficiencies and potentially lower haulage costs, such freight exchanges have also become a useful tool for fraudsters, as many forwarders in checking counterparties are guided only by the rating within the platform often overlooking the simplest tricks in the form of manipulated email addresses, for example. Such fraudulent activity not only presents a risk to the theft of cargo but also an existential threat to small operators through reputational damage.

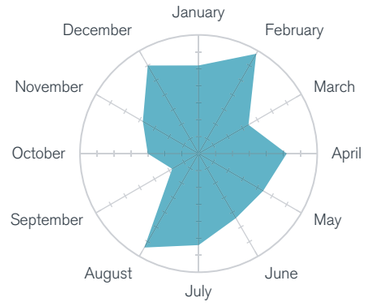
Cargo theft by federal district



Theft by month
2019



Theft by month
2020



Food & beverage

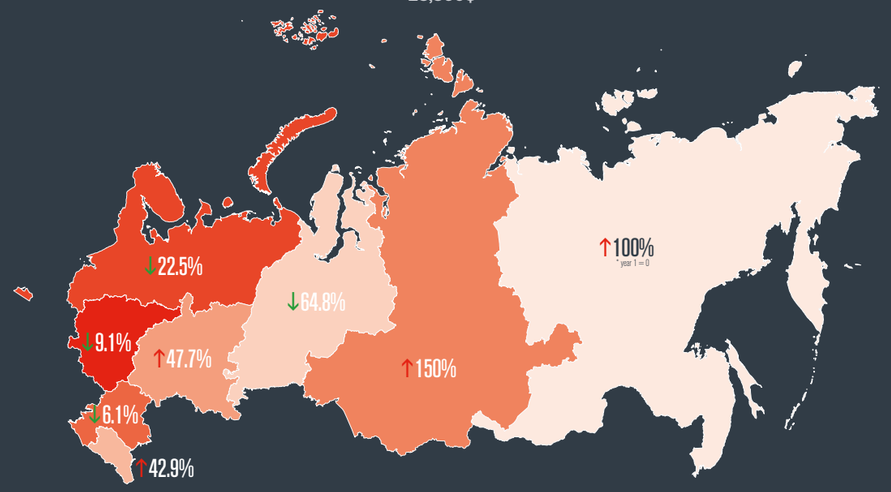
In line with the overall data, the number of thefts of food and beverage cargoes in 2020 reduced in frequency, by approximately 32%. The average value of stolen food and beverage cargoes also dropped from RUR2,748,560 in 2019 to RUR2,145,060 in 2020.

Average value

↓21.96%

2019 2,748,560₽
36,918$

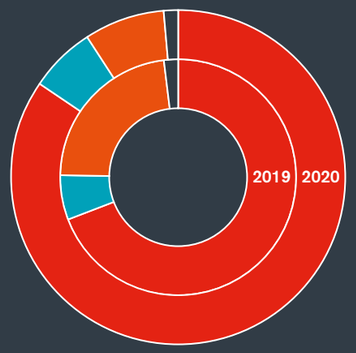
2020 2,145,060₽
28,806$



Modus operandi

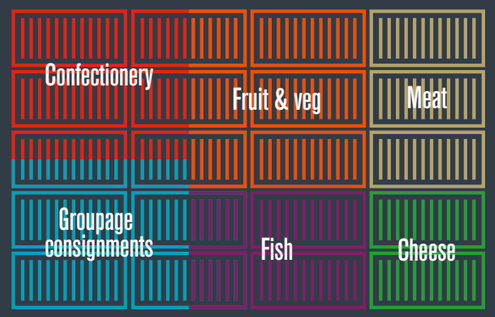
Food and beverage cargo thefts witnessed a similar shift in the modus operandi of the thieves during 2020. Incidents of theft from parked trucks reduced year on year, incidents primarily involving forged documents witnessed a sharp reduction from 22.8% to 7.7%. Incidents where thieves accessed the cargo under legitimate auspices to deliver the cargo to an undisclosed location spiked through the same period from 69% to 85%.

Individual commodities targeted within the food and beverage cargo group remained largely unchanged. Staples such as meat, fish, fruit and vegetables unsurprisingly remained in the top six in 2019 through 2020. Confectionery and groupage consignments were similarly targeted in both years. These cargoes will all have a wide market, a sustainable value return for the thieves and are consumable, so the longevity of risk to the thieves is finite, making them an attractive proposition.



	2019		2020
Unloaded at unspecified place	69.3%	↑	84.7%
Theft in parking lot	6.2%	↑	6.4%
Forged documents	22.8%	↓	7.7%
Other	1.7%	↓	1.2%

Most frequently targeted commodities



Major incident

22 December 2020 a full truck load of confectionery product valued at RUR1,753,000 was stolen in Kursk on the way to Ekaterinburg by a fraudulent pick-up. To get access to the cargo criminals used a legitimate account on a major freight exchange. The driver produced a set of forged identifications. After the truck dispatch the mobile numbers of both the dispatch and the driver were switched off. The cargo did not reach the destination. Six days later the same fake driver's identification was used in a different fraud scheme in the Food & Beverage category in the Tver region.

Metals & cable product

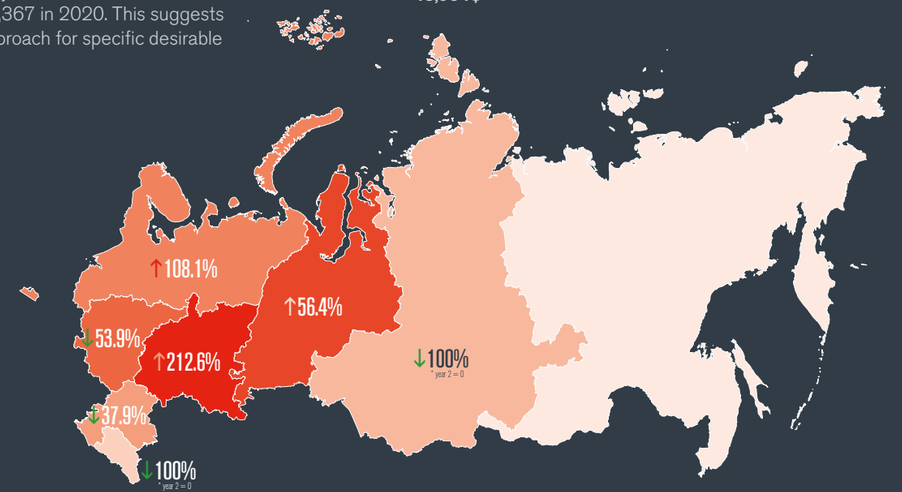
Thefts of metals during 2020 reduced significantly compared to 2019, a reduction of 68%. The average value of metal thefts in contrast rose sharply from RUR2,089,164 in 2019 to RUR3,270,367 in 2020. This suggests a more targeted approach for specific desirable commodities.

Average value

↑56.45%

2019 2,089,164₽
28,078$

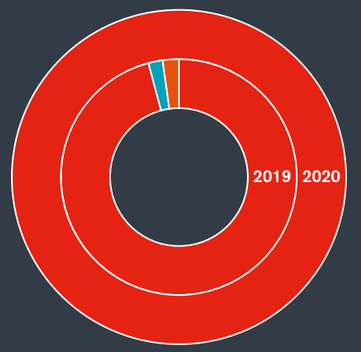
2020 3,270,367₽
43,904$



Modus operandi

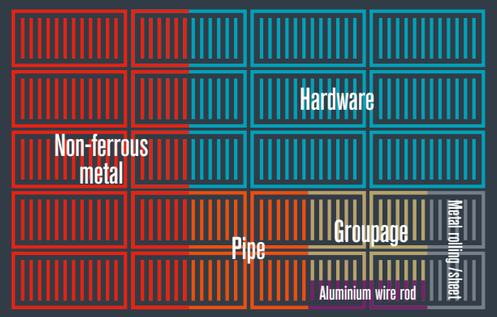
The modus operandi of thieves targeting metals continued to focus on legitimately accessing cargo and unloading at undisclosed locations during transit. All incidents in 2020 involved this type of fraud with all other strategies falling away. This again illustrates a focused and targeted approach by the thieves.

Non-ferrous metals remained the most targeted commodity within this cargo category in both 2019 and 2020. Hardware, metal rolling/sheet and metal pipe all remained within the top six commodities through the period.



	2019		2020
Unloaded at unspecified place	96%	↑	100%
Theft in parking lot	2%	↓	-
Forged documents	2%	↓	-

Most frequently targeted commodities



Major incident

A full truck load of non-ferrous metal was stolen in Urals region on 30 April 2020 on the way to Ishim, Tuymen region, the value RUR10,000,000. Criminals used driver's diverting tactic to access the cargo. After leaving the premises of the shipper the driver switched off his mobile phone and followed the instructions of 'unknown' persons to drive to unauthorized location to unload the goods.

Alcohol

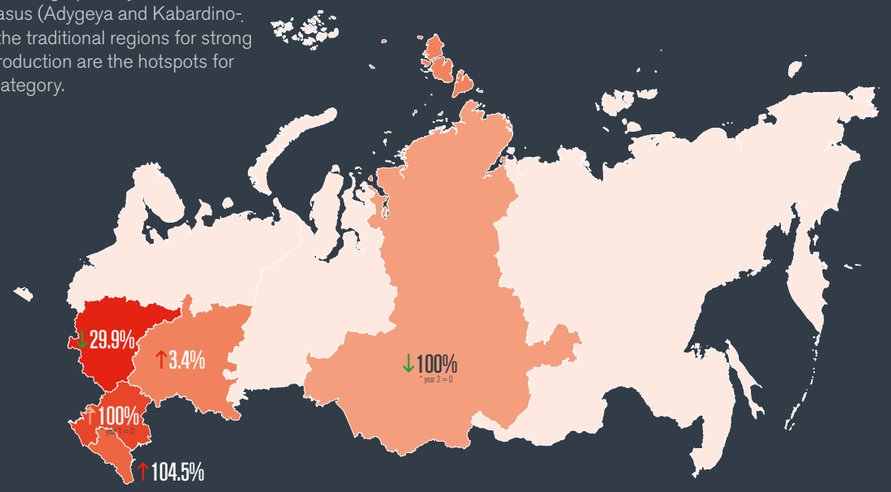
In terms of cost, the theft of alcoholic beverages accounted for almost 3% of the stolen goods in Russia in 2020. Despite the increased alcohol consumption during lockdown periods, reported incidents reflect a downward trend in comparison to 2019 where the overall value of stolen alcohol was approximately double. Geographically the Moscow and the North Caucasus (Adygeya and Kabardino-Balkaria) which are the traditional regions for strong spirits and alcohol production are the hotspots for cargo thefts in this category.

Average value

↓10.17%

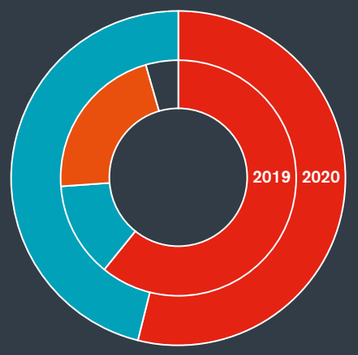
2019 2,261,950₽ / 30,692$

2020 2,022,841₽ / 27,694$



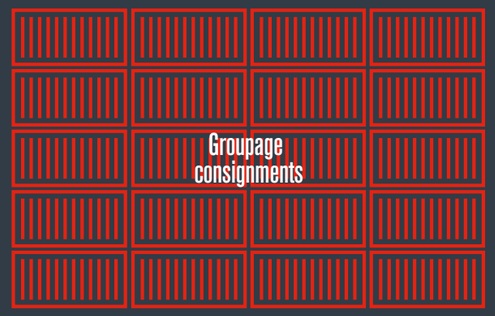
Modus operandi

There are three seasonal peaks for alcohol-related thefts in May, July-August and December. In 54% of incidents, criminal gangs used fraudulent schemes; the remaining 46% were stolen from trucks during overnight parking periods. Usually, the victims of cargo crime in this category of goods are alcohol manufacturers as in most of the cases they supply retail networks by employing freight forwarders who generally subcontract orders to multiple third parties via freight exchange facilities. Criminal groups closely monitor the situation on the freight exchange site and are ready to present an attractive freight offering to secure the order.



	2019		2020
Unloaded at unspecified place	61.0%	↓	54.0%
Theft in parking lot	13.0%	↑	46.0%
Forged documents	21.7%	↓	-
Other	4.3%	↓	-

Most frequently targeted commodities



Major incident

16 July 2020 a truckload of alcohol was stolen by fraudulent means in Selyatino, Moscow region valued at RUR 4.138.264. After leaving the factory premises, the driver received a call on his mobile and followed the offenders' instruction to unload cargo in unauthorized location.

Car parts & tyres

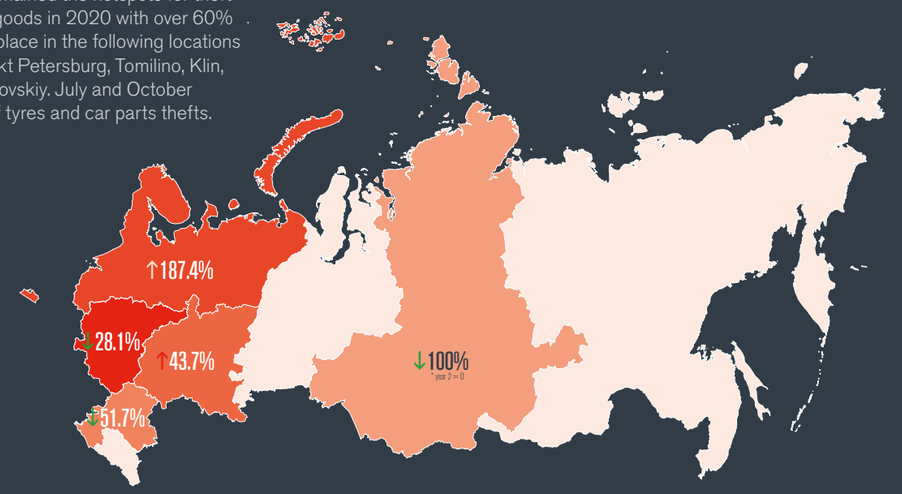
In 2020, the share of thefts of tyres and car components represented 8.9% of the total volume of stolen goods in Russia. In total IMPACT noted 22 major incidents, equal to 2019. However, the overall value has increased to RUR 65.300.000 representing a 25% increase on 2019. The average value increased by 16% year on year to RUR 2.800.000. Moscow suburban area and Leningrad oblast remained the hotspots for theft of this category of goods in 2020 with over 60% of incidents taking place in the following locations – Moscow city, Sankt Petersburg, Tomilino, Klin, Domodedovo, Zhukovskiy. July and October witnessed spikes of tyres and car parts thefts.

Average value

↑44.34%

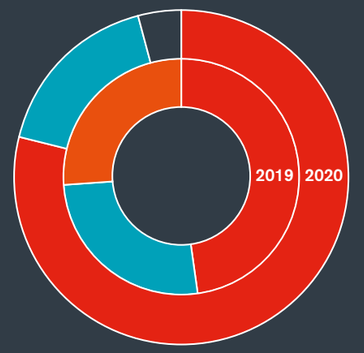
2019 2,354,921₽ / 31,968$

2020 3,401,859₽ / 46,105$



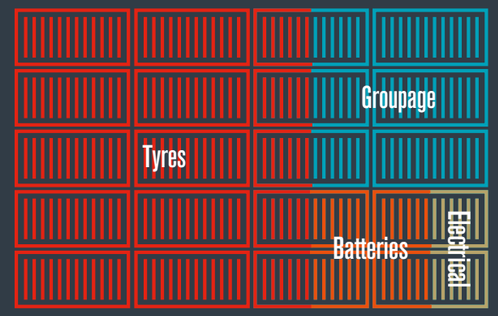
Modus operandi

Tyres and car parts are equally targeted with both primary modus operandi. Theft in transit – 21%, fraudulent pick up – 79%. Since the latter method usually involves full truck loss, it represents the bigger challenge for freight forwarders who are the main victims of this type of crime, despite measurable and robust security controls imposed to prevent losses. Unloading in unauthorized locations by "legal" front drivers is the most popular technique that organized criminal gangs are using to steal this type of cargo. In a series of fraudulent pickups, which typically take place at the beginning of the week, involving transits expected to take up to 3 to 5 days, several loads of tyres and car parts were stolen in Russia in 2020.



	2019		2020
Unloaded at unspecified place	48.0%	↑	79.0%
Theft in parking lot	26.0%	↓	17.0%
Forged documents	26.0%	↓	-
Hijacking	-	↑	4.0%

Most frequently targeted commodities



Major incident

On 31 July 2020, a full truckload was stolen from a manufacturer in Nizhnekamsk, Tatarstan. The value of the lost goods was RUR 4.600.000. After leaving the factory premises the driver, violating security protocols, followed phone instructions of 'unidentified' persons and unloaded goods in unauthorized location.

Electronics & home appliances

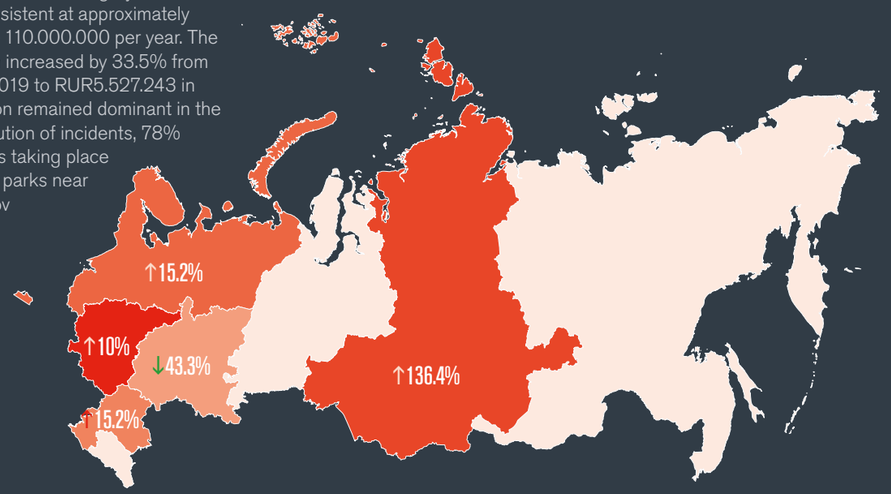
Electronics and home appliances remained one of the most targeted commodities in 2020. Accounting by value for up to 8% of stolen cargo in Russia. The total number of incidents recorded by IMPACT was slightly down in 2020 versus 2019. The total value of this category of stolen goods remained consistent at approximately RUR100.000.000 – 110.000.000 per year. The average value stolen increased by 33.5% from RUR3.900.000 in 2019 to RUR5.527.243 in 2020. Moscow region remained dominant in the geographical distribution of incidents, 78% of recorded incidents taking place at the large logistics parks near Marushkino, Chekhov and Novoselki.

Average value

↑33.55%

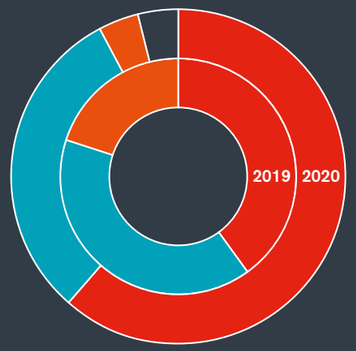
2019 4,131,763₽ / 56,101$

2020 5,527,243₽ / 74,795$



Modus operandi

Fraudulent pickups were employed in 65% of the incidents. Theft from trucks while parked during overnight stops accounted for the remaining incidents. Traditionally, the main victims of the criminal attacks are the larger national retail networks who historically have not recognized emerging threats and have low awareness levels of the modus operandi of the criminals. Despite security controls that retailers put in place for their selected logistics providers, organized criminals infiltrate in their supply chains by forging identity of legitimate carriers, buying their accounts in the freight exchanges and creating fake companies. Although this tactic is more resource and time consuming for the criminals, the larger return on investment from a successful attack, far outweighs the risks of being caught by the authorities. 2020 witnessed three distinct seasonal peaks for home appliances thefts in April, August and October-November.



	2019		2020
Unloaded at unspecified place	40.0%	↑	61.6%
Theft in parking lot	40.0%	↓	30.8%
Forged documents	20.0%	↓	3.80%
Other	-	↑	3.80%

Most frequently targeted commodities

⚠ ***Major incident***

On 12 August, four full truckloads were stolen in a single day from Novoselki logistic park in a large fraudulent scheme by employing four legitimate drivers and trucks dispatched by a third-party forwarder (criminal) subcontracted on a freight exchange. Total loss in this incident exceeded RUR20.000.000. The cargo never reached the intended destinations in Urals and Siberia and was not recovered.

Cosmetics, hygiene & household chemicals

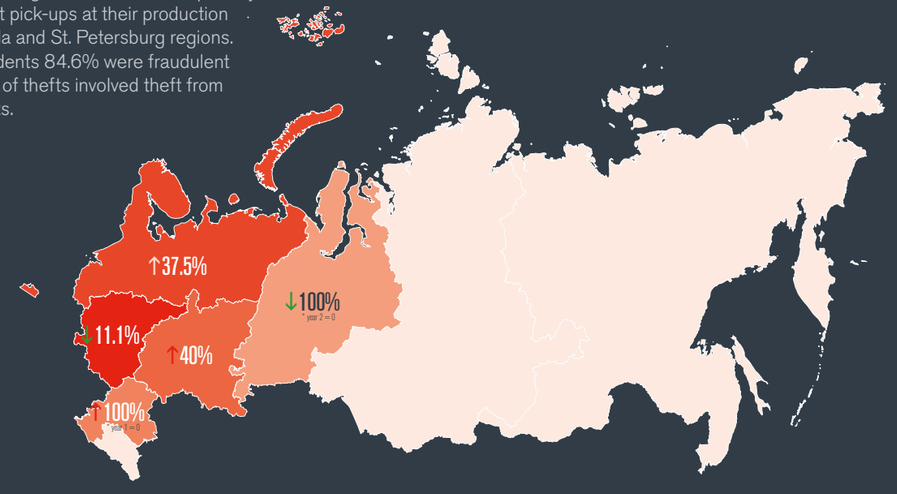
The theft of cosmetics, hygiene and household chemicals accounts for 4.4% of all cargo stolen in Russia. Despite overall drop in consumer demand in 2020, this category was still targeted by organized crime with various fraud tactics. Major global manufacturers operating in Russia were the primary victims of fraudulent pick-ups at their production sites in Moscow, Tula and St. Petersburg regions. The majority of incidents 84.6% were fraudulent attacks with 15.5% of thefts involved theft from trucks in parking lots.

Average value

↓2.57%

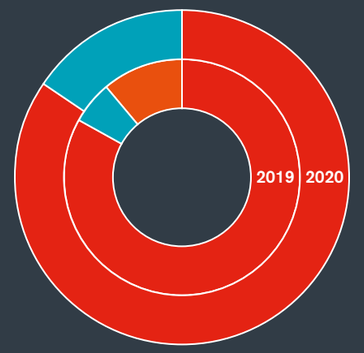
2019 3,668,244₽ / 49,792$

2020 3,581,036₽ / 48,416$



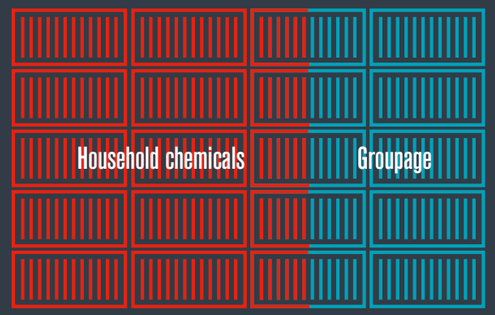
Modus operandi

Despite many manufacturers of cosmetics and hygiene products having sophisticated security measures in place, the current modus operandi employed by criminals allow them to overcome imposed management controls. Shipments of this category of goods are frequently placed in the open freight exchange platforms, where criminals can easily access them; offering favourable freight rates and producing legitimate truck and driver identification.



	2019		2020
Unloaded at unspecified place	83.3%	↑	84.6%
Theft in parking lot	5.6%	↑	15.4%
Forged documents	11.1%	↓	-

Most frequently targeted commodities



⚠ ***Major incident***

Two full truckloads of cosmetics and household chemicals were stolen in December 2020 from a major international manufacturer in a series of fraudulent pickups near Electrougli, Noginsk area, Moscow oblast valued at RUR5.000.000. Two drivers produced their identification and shipping documents and were loaded to deliver the goods intended for Novosibirsk and Krasnoyarsk. After leaving the load point, the drivers' mobile numbers stopped responding, any attempts to restore contact with them were unsuccessful. The goods never reached the destinations.

Industrial equipment & construction materials

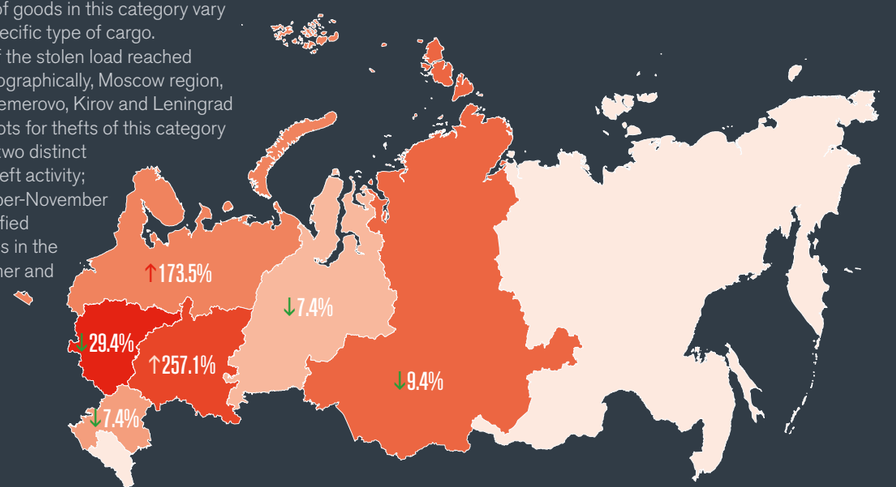
One of the most vulnerable goods category in terms of theft risks is Industrial equipment & Construction materials, which accounts for 11.5% of all cargo losses in Russia in terms of value. Despite COVID-19 restrictions in 2020, IMPACT registered 32 incidents in this category representing an increase on 2019. The value of goods in this category vary depending on the specific type of cargo.
The average value of the stolen load reached RUR 3.294.736. Geographically, Moscow region, Nizhniy Novgorod, Kemerovo, Kirov and Leningrad region are the hotspots for thefts of this category of goods. There are two distinct seasonal peaks in theft activity; May-June and October-November influenced by intensified construction activities in the country during summer and late autumn.

Average value

↑35.85%

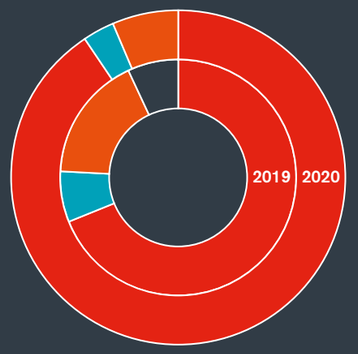
2019 2,423,187₽ / 32,705$

2020 3,294,736₽ / 44,389$



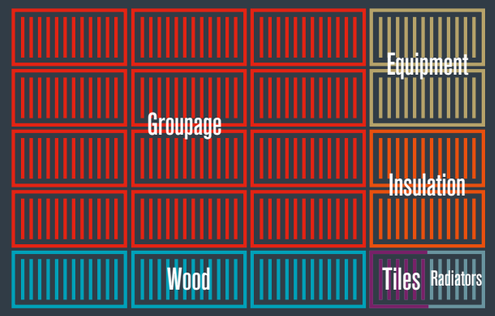
Modus operandi

Traditionally the victims in this category are manufacturers (industrial equipment) and retail (construction materials). Typically, awareness of the threat and appropriate mitigation strategies is low in this sector. Fraudulent tactics prevail accounting for 90% of recorded incidents. Given the opportunity of lower security controls, offenders often use less resource-consuming schemes in attacking cargoes in this category. Practically all orders in this category are placed in the freight exchange where offenders, represented by legitimate forwarding agency (bought or newly created) give shippers the most favourable quotes. "Legitimate" drivers collect the goods and will duly follow criminals' instructions to unload the cargo in an unauthorized location.



	2019		2020
Unloaded at unspecified place	69.0%	↑	90.6%
Theft in parking lot	6.9%	↓	3.2%
Forged documents	17.2%	↓	6.2%
Other	6.9%	↓	-

Most frequently targeted commodities



Major incident

On 18 November 2020, having collected a full truck load of industrial equipment valued at RUR17.000.000, the driver on the route Tarasovka, Moscow region to Khabarovsk, Far East, unloaded the cargo in the Moscow metropolitan area under the instructions of an "unknown" person. IMPACT notes that during the police investigation the driver acts as a victim of the fraudsters, but was known to have previously participated in similar cases.

Clothes & footwear

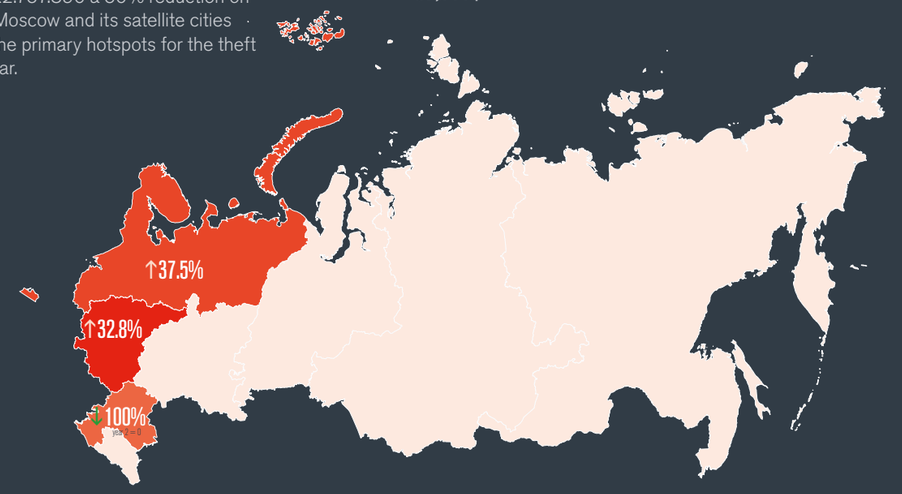
IMPACT notes a gradual yearly reduction of cargo losses in Clothes & Footwear category in Russia. In 2020, its share dropped in the rating of most targeted commodities down to 2.6%. Our records feature only nine recorded incidents with a total stolen value of RUR24.911.014. The average value of a loss fell to RUR2.767.890 a 50% reduction on the 2019 average. Moscow and its satellite cities within 50km were the primary hotspots for the theft of clothes & footwear.

Average value

↓49.84%

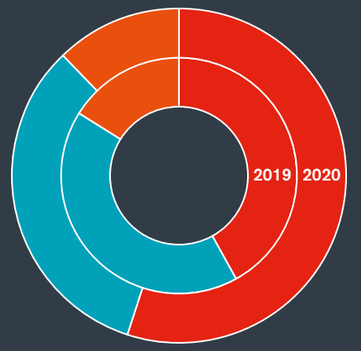
2019 5,520,304₽ / 73,966$

2020 2,767,890₽ / 37,111$



Modus operandi

IMPACT attributes the decrease of thefts in the Clothes & Footwear category to generally higher risk awareness and transport security measures imposed by manufacturers and their logistics providers. This fact is supported by the lower frequency of fraudulent schemes used to steal this type of cargo (fraud - 55%, theft – 33%) compared to other categories. As most of the branded clothing and footwear is imported in Russia via St. Petersburg's seaport in containers, criminals employed the tactics of manipulating the seals during transit, colluding with drivers. There were reports that in Tver region thieves operated several shop floors where they partially unloaded containers by manipulating seals leaving no trace of intervention. Existing evidence suggests this method was used in dozens of thefts alongside St. Petersburg – Moscow motorway in 2020.



	2019		2020
Unloaded at unspecified place	42.0%	↑	55.0%
Theft in parking lot	42.0%	↓	33.0%
Forged documents	16.0%	↓	12.0%

Most frequently targeted commodities

Major incident

IMPACT noted a report of the Tver region's Police department about the theft of branded clothing valued at RUR250.000, stolen from a truck in the Spirovsky district of the Tver region on 8 September 2020. One of the largest clothing retailers in Europe supplied its goods to Russian hypermarkets. Police detained the suspects who were residents of the Belgorod region, 33 and 34 years old. One of the suspects worked as a freight forwarder driver in a transport company.

A focus on fraud

Data from 2020 highlights that perpetrators of cargo theft in Russia rely heavily on fraud as a means of accessing cargo, this in contrast to many countries. The modus operandi of the criminal organisations are distinct and fall into two primary categories.

1. Driver being diverted by phone to unload at unauthorized location
2. The use of fraudulent identity to access cargo

All fraud related theft incidents require an element of inside industry knowledge to be effective. The ingenuity of the fraudsters is remarkable. They have sound knowledge of how the supply chain operates, what the important documents are, what they look like, what information they should contain, what size and type of vehicle they require to collect the goods and having a well maintained vehicle with a qualified driver who is operating within the legal framework. In many ways, the criminals are operating extremely efficient logistics operations.

Aside from stealing the cargo, evading detection is a primary focus for the fraudster. One should not forget that preparation on the criminal's part is a very cost effective undertaking. The prevalence of the internet affords straightforward access to vast data sources, allowing access to many instructive data points. Preparation is key for the criminal organisations, profiling vehicle movements, profiling individuals and the way cargoes are entered into the supply chain, how and when.

The sophistication of the criminal organisations in this context is often underestimated. Detection of these incidents as they unfold is increasingly difficult for legitimate stakeholders. There is importance therefore in raising awareness of the most prevalent modus operandi and explore ways that stakeholders can identify red flags and protect their business and the cargo they take into their care, custody and control.

In this section of the report, we will explore in detail the primary modus operandi and highlight the critical milestones through the process.

Fake carriers

Creating a persona impersonating a legitimate haulier is a tactic widely used by the criminals responsible for cargo theft. It is relatively simple to generate false email addresses, contact details and documents and, where sufficient due diligence is not undertaken, stakeholders can fall victim to this type of fraud.

Using smoke screens provided by online freight exchange platforms, locally devised freight distribution channels or simply presenting themselves at the collection point, fraudsters will monitor activity including volumes, frequency, the type of cargo and importantly the uptake of cargo by legitimate stakeholders. Where for example a time sensitive delivery remains available for collection, the nearer to the deadline, the less likely due diligence will be undertaken in the event that a haulier presents themselves to complete the job. There are also many cases where having obtained valuable information, a fake carrier presents himself or herself at a depot to collect a cargo.

The fraudster will strike when there is the least risk of apprehension. In presenting their solution, experience suggests that they will approach the legitimate stakeholder in one of three ways:

- Posing as a fictitious company. In such circumstances, they may only be able to offer a mobile contact number, a free mail email address and limited documents proving their legitimacy. They may have prepared fictitious documents, which in the absence of scrutiny might pass checks.
- Posing as a legitimate company, fraudulently. Fraudsters may steal the identity of a legitimate or well-known carrier. They may be able to prepare fictitious documents using the legitimate carriers' brand logo and generate similar but fake email addresses to reduce the chances of detection. Given your likely trust in a recognisable brand, you may elect to take very few, if any checks.
- Acting as a legitimate company with fraudulent intentions. The fraudster may have legitimately purchased a small or failing company and continue to trade under a trusted brand with fraudulent intentions. These circumstances can be difficult to detect, however, being mindful of changes in key personnel/contacts can be a leading indicator.

Case study

How it happens

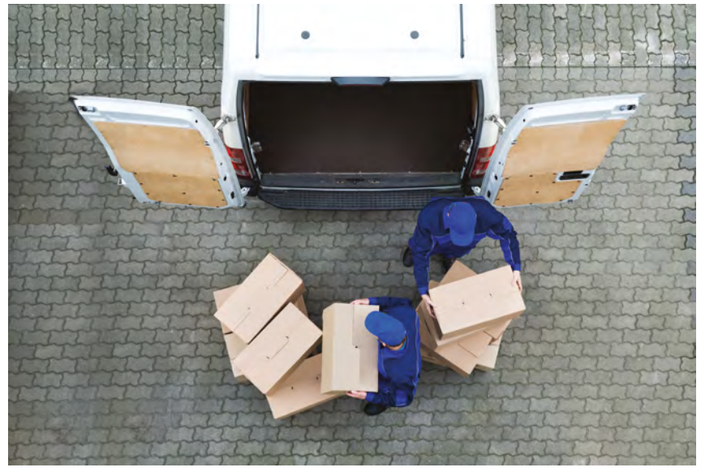
Coolmart, a national online retailer has a wide regional network of fulfilment centres supported by extensive transport operations. A strong pool of logistics service providers, including leading international brands undertake deliveries.

One of the providers, LN Forwarding, a local Russian branch of one of the world largest 3PL operators, was selected to move full truckloads on several primary lanes from Coolmart's Moscow central distribution centre to Urals and Volga regions. In peak periods the shipping volume allocated to LN Forwarding reached 15 trucks per day.

During one peak period, LN Forwarding was running out of vetted subcontractors' haulage capacity and to meet customer demand, decided to take a risk and outsourced trucks on an open freight exchange. An organized crime gang immediately identified the security gap and stole two full truck loads in one day worth RUR57,000,000. The criminals used a fraudulent pick up method involving a legitimate carrier profile on the freight exchange and forged driver identifications.

A complex argument evolved where each party sued the other, firstly for the value of the lost cargo and then a counter claim for unpaid freight fees. The decision of the Court was that each party should compensate the other in the amounts claimed.

Post incident investigations identified that the entity LN Forwarding involved in the case, was actually a clone of a well-known logistics operator in Russia. This came as an unwelcome surprise to all involved. No recovery was possible for the cargo owner, who soon after the loss filed for bankruptcy. The legitimate LN Forwarding business was also negatively impacted as their reputation was damaged by association with the loss through various media channels



"The entity awarded the freight contract was neither a carrier nor a forwarder, in business terms it didn't exist."

Case study

How it happens

MLY Clothing operate a large distribution centre in St Petersburg. There are on average 150 truck movements each day, around 50 inbound deliveries unloaded and 100 outbound deliveries loaded for distribution.

In the build up to Chinese New Year volumes peak as the Chinese suppliers build sufficient stock in preparation for the annual shut down. The distribution centre is working beyond expected volumes and everyone is under pressure to ensure that key performance indicator targets are met. Thursday is expected to be the peak of the busy period, 150 outbound trailers are due to be loaded through the 24 hour period (one every ten minutes). Additional personnel will be on duty, any delays to the planned activities will be catastrophic in completing all of the required work.

“The chances of apprehending those responsible and recovering the cargo are remote.”

At 0430 on Thursday, ABC Haulage arrive at the distribution centre with their truck, the driver proceeds to the traffic office announcing his arrival. The driver states that he is on site to collect an urgent load for delivery to London, but does not have the specific load number. By 0430, the distribution centre is already extremely busy. The driver states that he is unable to reach his employer to obtain the load number, as they are not due to arrive in the office for several hours. The clerk at the distribution centre, knowing that there is not a moment to lose attempts to assist by locating all loads due to be loaded for London that day, of which there are three. The clerk then discusses these loads with the ABC Haulage driver with a view to identify which load he is on site to collect.

The ABC Haulage driver states that he recognises one of the three loads to be the one he is to collect and arrangements are made to book him in. By 0630, the cargo has been loaded to ABC Haulage’s trailer and the driver leaves the distribution centre.

ABC Haulage were a fraudulent company, the fraudsters had been able to identify a particularly busy period and a vulnerable time of day to attack. By monitoring previous shipments, they were sufficiently empowered to expect with some certainty that there would be a load destined for London. While they did not possess particular load details, they were able to leverage the fact that the distribution centre was extremely busy to pressure the clerk into unwittingly assist them in accessing the load.

When such frauds take place, the criminals usually have several hours if not days before the alarm is raised. It is typically only when the delivery with the consignee does not take place that questions are asked and the fraud becomes known. The criminals have sufficient time to drive their vehicle to an undisclosed location that might be in a different country. They have time if required to change the licence plates of the vehicle. They have time to destroy temporary mobile phones or free mail email accounts. All of which makes it extremely difficult to track and locate the cargo, driver or truck. Typically, by the time this type of crime is identified the chances of apprehending those responsible and recovering the cargo are remote.

Loss prevention guidance

Awareness and training

One of the first and most important aspects of mitigating this type of risk is awareness training for those involved in all aspects of the supply chain. From the driver, the clerk at the logistics operator through to the clerk at the distribution centre. All need to have general awareness of the risks and be empowered where possible to identify the red flags. A key component of the training should focus on the level of preparation criminals undertake and that the attack will typically come during very busy periods or public holidays when they are more likely to be able to evade strict procedures.

Processes and escalation

Develop robust processes to verify identity. The importance of completing these processes needs to be stressed to all who are expected to undertake them. Whether it be verifying the identity of a prospective sub-contractor or the identity of a haulage company presenting themselves at a distribution centre. The processes should be sufficient to identify red flags while being proportionate, ensuring that they are strictly followed even through the busiest operational periods. Remember, criminals will profile a selected target extensively and select the most inopportune moment for the legitimate stakeholder, increasing their likelihood of success and avoiding apprehension.

Where discrepancies are identified, it is critical to have a clear escalation process in place to ensure that any final decision is made by a person with sufficient authority within the business. This can serve to allow those who are not emotionally tied to performance to make informed decisions.

Standards and technology

Applying industry security standards, specifically TAPA Trucking Security Requirements, can significantly reduce risks of fraud and traditional theft in the local supply chains. TAPA Standards can be used in business/security agreements (contracts) between Shippers and their Logistics Service Providers as a common language to avoid misinterpretation and gaps in security processes.

Widely available technological solutions for truck monitoring, alarm escalation and intervention should become a central element and key to success in preventing fraudulent attacks as it provides for better transparency, control and protection, as well as enabling efficient resource allocation in building security programs

Due diligence

Performing sufficient due diligence checks will assist businesses to protect themselves and the cargo that they take into their care, custody and control from this type of risk.

While not exhaustive, below are a number of items that operators could consider:

- Full legal name and registered address of the supplier
- Details of other branches (nationally or internationally)
- Contact details (telephone and email)
- Web address
- Verify ownership (taking account of regulations, such as sanctions, as appropriate)
- Company registration number
- Date of company registration
- Insurance details/policies
- Tax (e.g. VAT) registration number
- Governmental or similar audit scheme (e.g. AEO) membership
- Key personnel and their roles

As well as security aspects, there are potential regulatory and safety components to undertaking sufficient due diligence. Is the contractor for example qualified to carry the cargo you require moving? Is the driver trained to carry dangerous goods?

Do not be pressured in to circumventing due diligence procedures. The fraudster will know that you are under time pressure and will rely up on this to avoid detection.

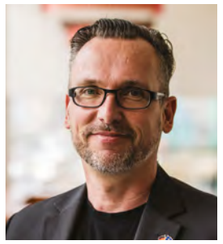
Meet the team

Ilya Smolentsev
Co-founder and Security advisor
IMPACT

contact@impact.ru.com
www.impact.ru.com

Mike Yarwood
Managing Director Loss Prevention
TT Club

michael.yarwood@thomasmiller.com
www.ttclub.com



Thorsten Neumann
President and CEO in the Europe,
Middle East and Africa Region,
Transported Asset Protection Association (TAPA)

thorsten.neumann@tapaemea.org
www.tapa-global.org

Kirill Berezov
Managing Director
Panditrans

kirill.berezov@panditrans.com
www.panditrans.com