Article

Flying in Cyberspace: Policing Global Travel Fraud

Alice Hutchings[*]

Abstract Airline tickets that have been obtained illicitly represent a truly global crime. The travel industry and law enforcement have been attempting to address travel fraud for some time. Airline tickets can be obtained using various cybercrime methods. They are traded and advertised on online blackmarkets and through fraudulent travel agencies. This research is qualitative in nature, informed by interviews with law enforcement and industry stakeholders, as well as the analysis of a marketplace where fraudulently obtained tickets are traded. This research considers: the nature of the criminal market for fraudulently obtained tickets, the involvement of co-offending and organized crime, the geographic nature of travel fraud, and the ways in which those supplying fraudulently obtained tickets try to avoid detection. Also considered is how the nature of travel fraud has changed over time, ways in which it may continue to change, and the challenges faced by law enforcement.

Introduction

This article considers the trade in fraudulently obtained airline tickets. Vulnerabilities and potential attack vectors that could affect the travel industry have been known for some time (Hasbrouck, 2001; Boggan, 2006; Jaroszewski, 2016; Nohl, 2016). However, there was previously little understanding about the various ways in which travel fraud actually occurs. Even those actively engaged in combating travel fraud will usually only see one part of the problem, due to its diverse nature.

As outlined in Hutchings (2018), compromised credit cards were previously the main way in which tickets were purchased illegitimately. However, offenders have displaced to other methods as their bookings have been identified and cancelled. In 2017, a man was sentenced for 4 years and 10 months in the USA, after being extradited from France, for using phishing techniques to obtain credentials for global distribution system companies, which provide booking services to travel agents. These credentials were used to issue fraudulent airline tickets, which were then sold or used personally by the offender and his accomplices. It is alleged that the value of the tickets that were obtained in such a way exceeded US$2 million, and that the majority were sold in West Africa (The United States Department of Justice, 2017). Additional methods to obtain tickets include the use of compromised loyalty point accounts, compromised business accounts, and to a lesser extent, identity fraud and voucher fraud (Hutchings, 2018).

[*]Department of Computer Science and Technology, University of Cambridge, Cambridge, UK.
E-mail: alice.hutchings@cl.cam.ac.uk

Policing, Volume 0, Number 0, pp. 1–16
doi:10.1093/police/pay063

In many instances, the traveller is not the one who actually obtained the ticket from the travel agent or airline. Fraudulently obtained airline tickets can be acquired knowingly or unwittingly by travellers (Hutchings, 2018). Online blackmarkets, which are used to trade in a variety of illegal products and services, contain advertisements for cheap tickets. Such blackmarkets are used for the anonymous trade in goods, including drugs and drug paraphernalia, credit card details, electronics, and weapons; and services, including those that enable fraudulent activities (Holt and Lampke, 2010; Motoyama *et al.*, 2011; Christin, 2013; Hutchings and Holt, 2015; Soska and Christin, 2015; Broséus *et al.*, 2016).

There are a number of vendors operating as travel agents on such sites, organizing plane tickets, hotel accommodation, and car rentals, advertised at around 25% of market price. Hutchings (2018) found complicit travellers and re-sellers use these marketplaces to purchase tickets. Victim travellers, who are not aware of the illicit origin of the ticket, may organize their travel through fake travel agencies advertising online, in classifieds and newspapers, the radio, and posters. Some travel agencies may not be completely fraudulent, but have insiders who have the opportunity to make bookings with stolen credit card data. Tickets are also traded through word-of-mouth, mainly through close-knit communities.

Europol have been running 'Global Airline Action Days' since 2013. Through these operations, which are run in cooperation with the airline, travel, and payment card industries, tickets that have been purchased using stolen credit card details are identified, and the travellers are detained. On average, each operation has resulted in 269 tickets being detected and 135 passengers being detained, although the numbers have been trending upwards over time (Europol, 2013; 2014a,b; 2015a,c; 2016; 2017a,b; 2018). In 2015, Europol estimated the loss to the airline industry as a result of fraudulent ticket purchases to be €1 billion (Europol, 2015a).

In addition to complicit travellers and victim travellers, those travelling on fraudulently obtained tickets include mules facilitating other criminal activities, as well as individuals being trafficked or smuggled. Regardless of the type of traveller, if detained by law enforcement during their journey, they will usually claim to be a victim traveller. However, it is estimated that the actual proportion of victim travellers is quite low (Hutchings, 2018). As travellers have plausible deniability, and due to the risks involved, they will travel with their own identification. Buyers on the blackmarkets are being coached on what to do if they are detained, and there are suggestions that they falsify receipts and communications to back up their claims of victimization. This causes problems for law enforcement when it comes to taking legal action against travellers, and subsequently, despite the high numbers of travellers being detained, there have been few prosecutions (Hutchings, 2018).

Travel fraud has been linked to a number of other crime types (Europol, 2015a; Hutchings, 2018). These include smuggling contraband, including drugs, cash, and cigarettes and tobacco. In some cases the movement of people has been linked to human trafficking, including for sexual exploitation, human smuggling, and illegal immigration. Property crimes include theft and robberies, including within airports, such as pickpocketing and organized shoplifting (Crime and Justice, 2014; Hutchings, 2018). In addition to smuggling cash, people can be transported to a country for the purpose of opening bank accounts, which are used for money laundering. And finally, further credit card fraud can be enabled through travel fraud, such as setting up skimmers and travelling to new destinations in order to use compromised card data. Links to terrorist groups, including financing and the movement of people, were alluded to, but are difficult to prove (Hutchings, 2018). There have also been indicators that some individuals who obtain the tickets are involved in organized crime. In October 2015, Europol reported that Romanian Police arrested 50 members of an organized crime group suspected of payment card fraud. It was alleged that the organization had used stolen card details to purchase plane tickets, among other things (Europol, 2015b).

While some fraudulently obtained tickets are detected and cancelled before they are flown, it is apparent that many travellers using these tickets travel successfully. In some cases, the booking is not detected before boarding, and sometimes it is not known to be fraudulent until some time later, when a chargeback is received. Those obtaining tickets use a variety of methods to try and minimize the likelihood that the booking will be detected before the flight takes place (Hutchings, 2018).

The aim of this research is to better understand the trade in, and use of, fraudulently obtained airline tickets. As a truly international crime, law enforcement agencies face considerable challenges in investigating and prosecuting these offences, therefore early detection and intervention is particularly important. Furthermore, very little is known about the economy surrounding this market, so identifying how the tickets are obtained will better inform the law enforcement, banking sector, and travel industry response. There is a serious risk that if people can evade existing controls, this crime type might become significantly more prevalent.

Research design and methods

Scope

The scope of this project has been limited to airline tickets obtained fraudulently from the travel industry. Therefore, relatively straightforward travel fraud that occurs in the open market, whereby the vendor receives payment but the buyer receives nothing in return, is explicitly excluded. Also excluded from the definition of travel fraud is ‘friendly fraud’, where a bank or airline customer claims that a genuine transaction on their account is fraudulent. It is further acknowledged that other travel industry segments experience similar fraudulent transactions, such as hotels and car hire companies. These are occasionally referred to within the context of this research, but are not the primary focus.

Research questions

This research aims to address a number of questions that relate to the trade of fraudulently obtained tickets. The first question is specific to the trade on anonymous online black markets, namely:

1. Are those who advertise or purchase tickets through anonymous online black markets also buying or selling other goods, such as illicit drugs or stolen payment information?
   Additional questions are addressed that are relevant to the travel fraud trade more generally:
2. What is the extent of the trade in fraudulently obtained tickets?
3. How do offenders operate and cooperate with each other?
4. What regions are involved in travel fraud?
5. What steps are taken to try and avoid detection?
6. How has travel fraud changed over time? How might it continue to change in the future?
7. What is the role of law enforcement in policing travel fraud, and what challenges do they face?

Methods

As the problem is being addressed from multiple angles (travel agents operating on online anonymous marketplaces and travellers with tickets obtained fraudulently), multiple data sources are used. These include interviews with the various stakeholders that identify, respond to, or are victims of travel fraud; and excerpts from an anonymous online black market where fraudulently obtained tickets are purchased. In addition to these formal methods, the researcher met with a number of law enforcement agents on an informal basis, made detailed notes, and consulted other research. Some information obtained during this inquiry could be used by offenders to improve their methods, or to help them avoid detection. While interesting, such information has not been included in this article as it is considered prejudicial.

Interviews. Interviews were completed with individuals (referred to herein as ‘participants’) who are familiar with various aspects of travel fraud. These include law enforcement, analysts, and industry partners (banks, airlines, and industry bodies) who actively detect and investigate fraudulently obtained tickets. Particular care was taken to include participants who were familiar with different aspects of travel fraud, such as the booking of the tickets, the interception of those that were travelling, and those familiar with the online trade of fraudulently obtained tickets. In total, 13 interviews were completed, with four participants from airlines, two participants held analyst roles, three were law enforcement agents, two were from industry bodies, one was from a financial institution, and a final participant provided insights from the hotel industry. Many of the participants were recruited through one of the analysts, who is familiar with the landscape, and has the relevant contacts. Further recruitment took place using a snowball sample, in that participants identified additional organizations and individuals to speak to, and through other law enforcement contacts. Interviews took place face-to-face, as well as by telephone and VoIP. Participants were recruited from the USA, Asia, and Europe.

The interviews were qualitative and semi-structured. An interview schedule was used, which outlined the topics to be canvassed, however, each interview was tailored to suit the participant, depending on the aspects of the trade that they were most familiar with. Questions explored the sale of, and travel on, fraudulently obtained tickets, and potential countermeasures.

Ethical clearance was granted, and participants were given an information sheet providing an overview of the research. Verbal consent was obtained, both for the interview to be recorded and for the data to be used for analysis. The interviews took between 24 and 101 min, with an average time of 66 min. All interviews were transcribed, excluding any information identifying the participant or specific third parties.

Marketplaces. A database of exchanges on one of the anonymous online black markets, which was identified as being the most utilized for travel fraud, was searched for a number of relevant terms. The search terms used were combinations from List A and List B detailed below, as well as the standalone search terms in List C. List A includes travel-related search terms; however, on their own these terms returned many listings that were not relevant to this project. List B allowed the results to be more specific to the travel fraud industry, and were designed to specifically elicit the feedback left by unsatisfied customers, who may have been intercepted by law enforcement, or were unsuccessful in their travel attempts. It was felt that these comments might be more forthright, and contain useful information that would help identify the methods used for this fraud type. List C includes a number of highly specific terms that are unlikely to be used out of context, that relate to the travel industry. The first three terms are names of specific global distribution systems, or GDS’, which are used by travel agencies for booking tickets. The Airlines Reporting Corporation (ARC) and International Air Transport Association (IATA) are industry bodies for the travel sector.

List A	List B	List C
Travel	Police	Amadeus
Airline	Europol	Sabre
Boarding pass	Ripper	Travelport
Flight	Scam	GDS
Hotel	Law enforcement	Global distribution system
Expedia	Cops	ARC
	Scammed	ARC
	Arrested	IATA
	Broker	IATA

The data consist of advertisements and forum discussions on the anonymous black market, including feedback from unsatisfied customers. Not all search terms or combinations returned matches; however, 47 unique threads were identified, covering periods from December 2014 to August 2016.

Analysis

The interview transcripts, forum content, and the researcher's notes were analysed qualitatively. Coding of the data was 'data-driven' (Gibbs, 2007), using NVivo, a qualitative data analysis program, to classify and sort the data.

Findings

Question 1: trade in other goods and services

The anonymous online black markets are used to trade in a variety of goods and services. It was believed that fraudulently obtained travel may be used to facilitate this market, such as drug trafficking. Furthermore, stolen data sold on the marketplaces, such as credit card information, can enable the fraudulent purchase of tickets. Both marketplace sellers and buyers are of interest, to see if each are buying and/or selling other goods and services.

Sellers selling other goods and services. Commonly found advertised with flight tickets are other travel services, such as hotel accommodation, car hire, and tours/activities. In addition to these travel-related products, some sellers trade in credit card data. One seller was selling tickets for UK flights that they claimed were not purchased using compromised credentials. A potential customer queried this, noting that the same seller was advertising UK fullz.[1] The marketplace seller claimed that the two products were unrelated. Notes relating to specific sellers indicated one was advertising PayPal accounts for the USA, Australia, and Spain, as well as credit card numbers for various UK banks. Another traded in credit cards, access to computers, software licensing keys, and e-gift cards. One seller also advertised UK credit card data, compromised online accounts at various financial institutions and retailers, compromised identities, fraud how-to guides, drugs, and a drop service.[2] Other sellers also advertised credit card data and drop services, as well as narcotics and cashout services.[3]

Sellers buying other goods and services. Another buyer notes that a seller, who also claims not to purchase tickets using compromised cards, had requested to buy fullz on another thread. Another seller had previously attempted to purchase a variety of online bank account credentials, personal information and scans of documents, hacking services to obtain access to a gambling site, fullz, and dumps.[4]

Buyers buying other goods and services. According to one of the analysts, some buyers of travel services also purchase credit card data. Some also purchase products and services related to other fraudulent activities they are engaged with. The example provided was reshipping scams, where buyers may also purchase label services[5] and mule services, as well as stolen credentials.

Buyers selling other goods and services. The only reference found of buyers selling other products related to re-sellers, who were on-selling the fraudulently obtained tickets.

[1] 'Fullz' refer to credit card data (card numbers and verification values) with further information associated with the account, including data relating to the account holder, such as name, address, date of birth, and PIN (Hutchings and Holt, 2015).

[2] 'Drop services' receive fraudulently purchased goods, and can exchange them for cash (Holt, 2013).

[3] 'Cashout services' turn ill-gotten gains into cash, such as using dumps encoded on to plastic cards to withdraw money or purchase goods for resale (Hutchings and Holt, 2015).

[4] 'Dumps' are data read from the magnetic stripes of credit cards, which can be used for creating credit card clones (Holt and Lampke, 2010).

[5] 'Label services' allow users to purchase and print postal service labels using compromised card data so that packages can be shipped and delivered at a low cost (Krebs, 2012).

This was evidenced by their reference to ‘clients’ when leaving feedback on the forums. It is possible the buyers do sell other products and services, but the data related to this was not captured by the methodology used.

Question 2: extent of trade

Amount of trade by sellers.

Various claims were made by the sellers about the amount of trade that they engaged in over time or across marketplaces. Some buyers also claimed to have travelled on a large number of fraudulently obtained tickets, or to have spent large sums with sellers. However, such claims may be boasts by sellers to increase their perceived popularity.

Size of the market.

Comments left by buyers and sellers in the marketplaces indicate that there is a demand for cheap tickets. Marketplace sellers refer to receiving ‘too many’, ‘an influx of’, and being ‘slammed with’ orders. However, advertisements for travel services make up a small proportion of sales on these marketplaces overall.

Overall cost to the provider.

In the US, an industry body identifies ‘a few dozen’ confirmed fraudulent tickets purchased each day through travel agencies, and for many of these, the travel has already occurred. In these cases, the travel agency incurs the loss, unless they are insolvent. One participant advised that it would be difficult to identify how much the airline had lost due to ticket fraud, as chargebacks could be received many months after the transaction, and some fraudulent transactions may not be identified at all. They also claimed that published loss figures were ‘guesstimates’. To illustrate these problems, the loss associated with just one compromised business account was estimated at around US$740,000, and took over a year to identify. Another participant from an airline advised that overall, fraud cost the company <1% of their income. They further noted that there had been no attempts to benchmark costs across the industry, and that these can be calculated in a variety of ways, including the amount detected and prevented, and the amount that was lost as travel occurred before the transaction could be reversed. In addition to the direct costs incurred due to fraud, there are indirect costs incurred when anticipating and responding to fraud incidents.

Number of loyalty points re-issued.

One method for fraudulently obtaining airline tickets is to compromise loyalty point accounts. One airline participant advised that per day they typically re-issue 200,000–500,000 loyalty points to compromised customer accounts, and recover a further 500,000 points. This indicates that this particular airline is detecting over half of the fraudulent redemption of loyalty points before the travel has taken place. Placing a monetary value on loyalty points is not straightforward, but potential ways to do this are the cost of the points, for those providers who enable additional points to be purchased, or the value of the products that the points can be redeemed for.

Question 3: co-offending and organized crime

There are many meanings associated with the term ‘organised crime’ (Hutchings, 2014), and there is a tendency to overestimate the extent that crimes are organised (Felson, 1994). However, whether it is organized crime or co-offending, it is important to understand how offenders operate and cooperate with each other. Many of the participants claimed that ticket fraud had elements of organized crime, and this may manifest in multiple ways.

Sellers and buyers.

In relation to travel fraud, the trade of tickets from one offender to another may itself by considered to be co-offending. Some re-sellers will develop business relationships with sellers, ensuring repeat business. The development of relationships in online marketplaces is gradual, as learning who to trust in untrustworthy environments can be costly (Holt *et al.*, 2016).

Sellers and data providers. As identified in Hutchings (2018), sellers themselves may not have compromised the accounts or data that they are using to fraudulently purchase or redeem the tickets. Therefore, they will have some kind of business relationship with the providers of these data and insiders within the travel industry. One marketplace seller also claimed that sellers were all in contact with each other, to ensure that problematic buyers were identified (however, other activity in the forums indicated that the sellers could be highly competitive). There were also indications that marketplace sellers were not sole operators, but involved the cooperation of several people, who book the tickets and provide customer support. There were some indications in the forum data of these relationships falling apart.

Buyers and travellers. In some cases, buyers are providing tickets to others for the purpose of committing further crimes. All of the crimes that are known or suspected to be related to fraudulently obtained tickets may also have elements of organized crime involvement. These include drug trafficking, human trafficking and human smuggling, shoplifting and pickpocketing at scale, smuggling cash and contraband, money laundering, and credit card fraud.

Question 4: regions

As a truly global fraud, regions in the world play an important part. On the forums, there were discussions about which parts of the world were more or less risky to depart from. Some marketplace sellers would only book flights leaving from some countries, while others advised that they were unable to book flights from certain regions.

Participants were asked what routes they saw, and where sellers were located. The mapped responses are shown in Fig. 1. There are some biases in the responses, as depending where the participant is based, they may be more or less likely to see certain locations and actors. Some participants also do not allow certain routes to be booked. Therefore, they believed that they were only seeing some segments of the fraudulently booked travel. For example, one participant was identifying a lot of domestic flights; however, it appeared that the passengers had flown into the USA on fraudulent tickets travelling with other carriers. The actors that sold and booked the flights were known or believed to be in Europe, West Africa, North and South America, and South Asia. There did not seem to be any relationship between the region of the seller and the type of method used. On the marketplaces, tickets were sold in a variety of languages, including English and Russian, although in some instances it was apparent that advertisements had been translated.

Many of the participants are familiar with patterns in the data that they saw. Some routes, including domestic flights in the USA, as well as international flights, are believed to be associated with drug smuggling. One participant is familiar with a route whereby individuals, potentially those being smuggled or trafficked, are departing from Haiti, into Ecuador, then their systems were picking up the same individuals moving from Mexico into the USA. This participant also saw many women travelling from Moscow into China, and hypothesized that they may be victims of trafficking. Another smuggling route is from Africa into Europe. Other participants associate travellers from Eastern Europe arriving into the USA with money laundering. Some travel is also seasonal, or based on large events. For example, one participant found that travel fraud into Brazil peaked during the 2014 World Cup. December is also associated with an increase in travel to warm locations, apparently to escape colder climes.

Question 5: steps taken to avoid detection

A successful journey is one that does not get cancelled, and where the traveller is not greeted by law enforcement. Some (but not all) of the steps that sellers and travellers take specifically to minimize the chances of detection are outlined.

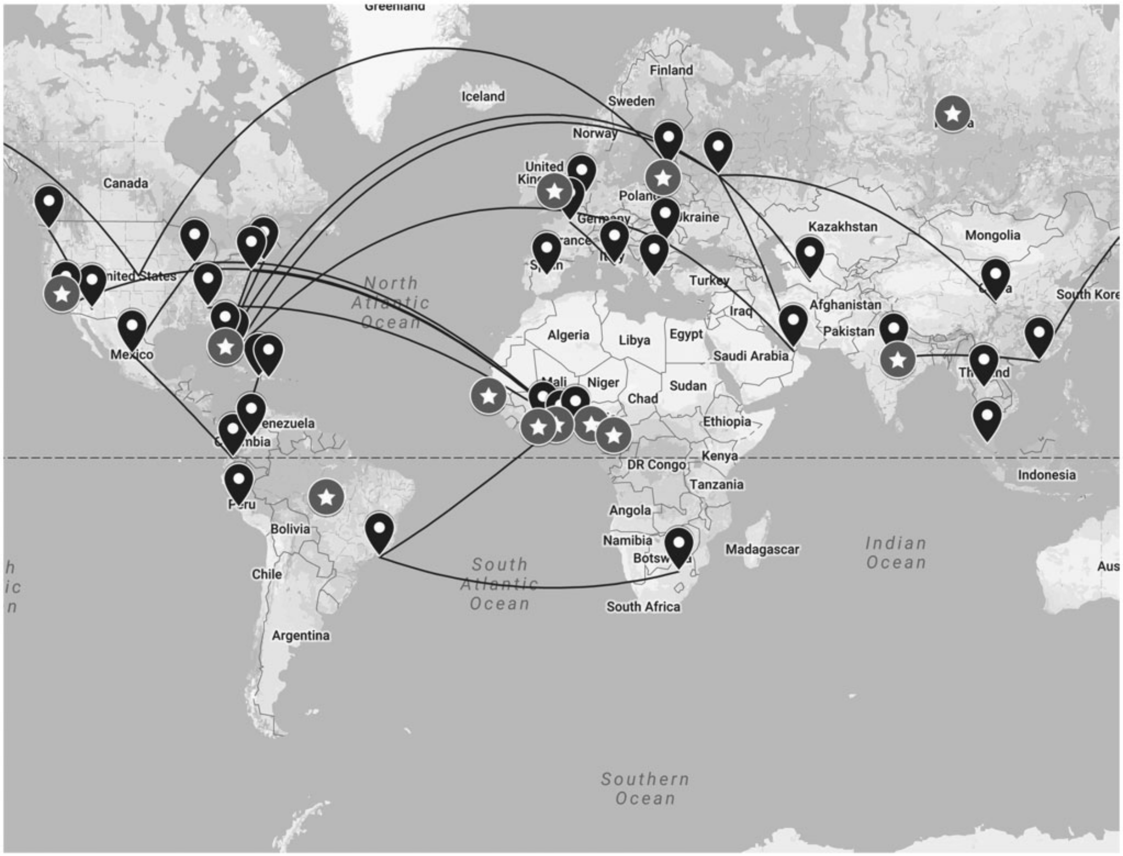

Figure 1: Map of identified routes and travel locations 📍 and sellers ★.

OpSec (operational security). Those buying tickets may take a number of operational security steps to avoid detection, in order to successfully purchase the ticket, but also to avoid the illegal purchase being linked back to them. Some of the precautions limit the chances that the seller will have possession of incriminating evidence if detected. In the marketplaces, many sellers request that screenshots be taken of the flight itinerary, that the screenshot be posted on a website where uploaded images will be deleted after a certain period of time, and that the link be sent to them. Some of these websites offer single use URLs, where the content is only served up the first time it is visited.

Other precautions taken by those booking the flights are to mask their IP address, and use VoIP services when making calls, so that it appears they are located elsewhere. They will also frequently change these details, to minimize the chances that their bookings are flagged. E-mail addresses used for bookings, or changed on compromised loyalty point accounts, are often completely fake, or disposable, temporary email addresses that are used just for one booking.

Purchasing through airlines or agents. Obtaining flights directly through the airline is seen as particularly risky, therefore many obtain them ‘indirectly’ through travel agencies. According to the chatter on the forums, the smaller travel agencies are less likely to pay for fraud detection systems. Bookings are still made directly through airlines using a variety of methods; however, there has been a recent trend towards travel agency bookings.

Purchasing online, in person, or by phone. Bookings are commonly made online, but some are also made by phone and in person. Advice was found on the forum indicating that purchasing through call centres is less risky than online bookings. When taking online bookings, the provider has access to data that may inform fraud risk, such as IP addresses and device fingerprints. A participant recounted a tale of someone audaciously taking stacks of cards to their airline desks and successfully, and repeatedly, purchasing last-minute tickets for people based all around the world.

One-way or return tickets. One participant hypothesized that those travelling on return tickets may be victim travellers who are unaware that they are travelling on fraudulently obtained tickets, but those on one-way tickets may be complicit in some way. However, other participants believed that return trip tickets were being purchased in order to make transactions appear less suspicious, with no intention of travelling the second flight. Furthermore, a return flight out may be booked for immigration purposes, and back-up flights may be booked, in case one is cancelled. These possibilities mean that there can be many more bookings, through different providers, than are actually used.

Time between booking and travelling. Although some airlines do not allow last minute bookings, it seems to be a common practice, and there are many people travelling on legitimately purchased tickets who require emergency travel. Fraudulently booked tickets were reportedly often booked shortly before the flight was due for departure, with one airline estimating that 80% of fraudulently obtained tickets were departing within 24 h. Booking shortly before flying limits the time available for scrutiny, for confirmation that a card has been used without authorization, and for the chargeback process to commence. These limitations are particularly pertinent when it comes to international flights, where the banks, airlines, and other parties may be all located in different time zones. However, as so many fraudulent bookings are made close to the point of departure, these can receive a higher score in fraud detection systems. The tension created by last-minute booking is evident on the forums, as flight bookers were eager for confirmation that the transaction will proceed. Some marketplace sellers advertised that they only made emergency bookings, for near departure.

Corruption. No discussion relating to corruption on the forums was found with the search terms used. However, an informal discussion indicated that it was a concern for some law enforcement. Furthermore, there was evidence that corruption had occurred in at least one instance relating to travel fraud. In this instance, a law enforcement officer was apparently extorting protection money from those who had travelled on fraudulently obtained tickets. Other potential avenues for corruption may be more systematic, such as providing tips when not to travel, or opportunistic, such as accepting a bribe rather than arresting or charging someone identified travelling fraudulently.

Question 6: change and future directions

One participant explained that when they started in the industry, they were mainly combatting embezzlement within travel agencies. It was only once this was under control that fraud involving illicitly obtained tickets was noticed as a problem. The future directions of travel fraud can be difficult to predict, as much of the current direction has taken advantage of presented opportunity. Therefore, it will depend much on the airline industry itself and how people use (and misuse) their services. This is illustrated by demonstrating how travel fraud has changed over time. Some possibilities where there will be opportunity for more criminal activity are explored, as well the possibilities opened up with the use of alternative currencies such as Bitcoin.

Opportunity for criminal activity. Travel is a service industry, and travel businesses are operating in a competitive environment, where there is a need for innovation to compete successfully. However, with each innovation, there can be new opportunities for exploitation. Despite participants having been in the industry for varying periods of time, they agreed that they had seen change in how travel fraud was committed. This was both short-term change, such as within the previous year, and long-term change, going back decades.

Travel on fraudulent tickets apparently used to involve the manipulation of paper tickets. However, this has changed with technology, with one airline participant advising that they had been experiencing online fraud ever since they had begun offering tickets for sale online. Similarly, loyalty point fraud had reportedly increased in line with the opportunity that loyalty point accounts presented. However, it is not just opportunity provided by the travel industry that affects the type of fraud, and how it is perpetrated, but also opportunities provided by other criminals. For instance, the availability of anonymous online black markets has provided a new forum to buy and sell fraudulently obtained tickets.

There are claims that travel fraud is becoming more sophisticated, as fraud methods become more advanced, and those purchasing tickets learn from experience how to circumvent fraud detection systems. On the other hand, it was noted that 'fraudsters are inherently lazy'. They are less likely to set up elaborate frauds, such as committing identity fraud to open up credit accounts, when compromised accounts are available en masse, and are relatively straightforward to abuse. While disrupting existing techniques may reduce the amount of tickets being obtained fraudulently, it may also lead to displacement and further innovation.

Displacement. Crime is considered to be displaced when it moves to alternative offence types, methods, locations, targets, times, or offenders as the result of prevention initiatives (Smith *et al.*, 2003). In relation to travel fraud, it is evident that displacement goes hand-in-hand with opportunity, particularly with the offence type used. As credit card fraud has become more difficult to perpetrate successfully, other methods are being utilized. Buyers are also displacing to new targets, moving from one ticket provider to another, once their purchases are detected and prevented. Furthermore, the methods for each offence type are changing. A participant described how they made it more difficult for loyalty point account compromise to take place over the phone, by providing training within their call centres, and subsequently saw the fraud moving back to online methods.

Potential future directions. There were some techniques that have been seen in relation to fraud that either had not been encountered in relation to travel fraud, or had not been detected. Phishing is one such technique, where scammers seek access to online accounts. This is typically perpetrated through spoofed emails, pretending to be from a service provider, requesting that the recipient enter their credentials. Phishing campaigns have targeted travel agencies, to gain access to booking services. However, participants advised that they had not encountered phishing campaigns targeting the general public. Potentially, this technique could be used to gain access to loyalty program accounts run by airlines.

Another potential area for capturing loyalty account credentials could be through malware, which can be configured to capture usernames and passwords from particular targets. Tajalizadehkhoob *et al.* (2014) explored target selection by examining 11,000 configuration files dating from January 2009 to March 2013 and relating to Zeus, a type of Trojan. The 2,131 botnets identified in this period had 2,412 unique targets. The web traffic and ranking organization Alexa categorized 32% of the targets as financial service providers and 11% as other industry segments, while 57% were uncategorized. However, for this research, none of the participants were aware of malware being used to harvest credentials for loyalty programs, although it was not ruled out.

Hutchings (2018) discusses the various ways insiders within organizations can facilitate travel fraud. However, not all participants were aware of malicious insiders that had operated within their own organizations (although they may have avoided detection). This may be an area for future criminal opportunity. Insiders may obtain employment at a targeted service provider, be targeted by those looking to sell fraudulently obtained tickets, abuse their access as the result of becoming discontent in their employment, or become tempted by presented opportunities and the potential perceived gains.

Some participants were concerned about the criminal opportunities that may be created with alternative currencies such as Bitcoin. Some European airlines are now accepting payments using Bitcoin, and chatter on the forums indicated that a travel agency in France also accepts this payment method. The participants did not know if these businesses had experienced any issues with Bitcoin transactions. However, participants had a variety of concerns about criminals making and accepting payments using Bitcoin.

The first concern relates to purchasing tickets from providers using Bitcoin. Airline tickets may be a way to convert Bitcoin obtained through criminal means, such as trading in illicit goods, into a commodity for re-sale. This method could also be used for money laundering, where victim travellers could purchase tickets through travel agencies, who use Bitcoin obtained through nefarious means, and accept the 'clean' funds in return. According to one law enforcement participant, Bitcoin was the preferred payment mechanism for cybercriminals in Europe. The forum chatter also suggested purchasing Bitcoin with compromised credit card data, and using these to purchase the tickets, in order to prevent the likelihood of detection. Furthermore, Bitcoin wallets can be compromised, just like other online accounts, and used fraudulently.

The second concern relates to the use of Bitcoin to accept payment for tickets obtained using other means. It is apparent that Bitcoin is already used as a payment method on the black market forums for this purpose. Another possibility is that fake travel agencies could operate on the clearnet, accepting Bitcoin from victim travellers, and finalizing the transaction using compromised card details.

The use of Bitcoin could be of an advantage to criminals, particularly when mixers and tumblers[6] are used to make it more difficult to trace criminal transactions. Furthermore, the lack of a chargeback facility could create an incentive problem for those accepting payments. Because they do not lose financially when fraud is detected, as they may with credit card transactions, there may be less incentive to detect suspicious transactions.

Question7: law enforcement

In some cases, law enforcement become involved, and detain and question those travelling on fraudulently obtained tickets. This may be part of the global airline action days, run with Europol and other industry and law enforcement partners, part of a focused investigation, or done on an *ad hoc* basis. Europol has taken the lead on this issue, coordinating the Global Airline Action Days since 2013. These have gradually expanded, to increase the number of jurisdictions involved.

As identifying who is truly a victim traveller is problematic, when a traveller is detained, they are rarely charged with any crime. These difficulties

[6] Mixers and tumblers are services designed to reduce the traceability of Bitcoin and other cryptocurrencies by mixing and redistributing coins from different sources (Meiklejohn and Mercer, 2018).

have not gone unnoticed on the forums. While they have shared media releases relating to the global action days, they also note that law enforcement are rarely involved, and if they are, it is the traveller, not the person who obtained the ticket, that is targeted:

> Although it looks like they ve [*sic*] arrested purchasers of said service but not the guys running the business in the first place . . . (blackmarket post).

However, participants indicated that law enforcement were starting to take more action in relation to travel fraud, and even when a passenger was detained with no charge, this ultimately causes some disruption to the person who had organized the ticket. There are a number of challenges that the travel industry and law enforcement need to overcome in order to better police travel fraud. Some of the issues include:

- The low dollar amount for one-off purchases. This has been noted in the forums, where actors reassure each other that the risk is low for this reason. Some participants said that they could only get law enforcement involved when losses started to reach multiple hundreds of thousands of dollars.
- Fraud is not seen as a priority for law enforcement. Furthermore, adding complex international aspects can make investigations unattractive to pursue.
- A lack of international contacts. Like many interactions in life, having trusted relationships can make communications easier. However, due to the global nature of travel fraud, making connections with law enforcement all around the globe, with different time zones and languages, can prove difficult. While airlines advised that they often have good relationships with their local law enforcement agencies, this is more difficult in non-local jurisdictions.
- Some policing agencies do not want to, or cannot, get involved in cases that do not directly relate to their own country, such as when an international traveller is arriving on an airline from another country, and the affected financial institution is also overseas.
- There can be local jurisdictional issues. For example, in some countries the police officers that work in airports have no jurisdiction over fraud matters.
- A lack of awareness about travel fraud. Many law enforcement officers are not versed in complex frauds, and there is little institutional knowledge about the problem. Even when law enforcement detains a traveller, they may not know the types of questions to ask.
- Problems with being able to charge those travelling. This issue is compounded when travellers are, or claim to be, victims who do not know that the ticket they are travelling on has been obtained illegally. Furthermore, some law enforcement are unlikely to charge someone with credit card fraud if they are not in physical possession of the card, even for card-not-present transactions.

There is also seldom any action taken after a flight has already occurred. Of course, this can be challenging for law enforcement, because in addition to the points covered above, the location and residence of the traveller can be difficult to identify. Detaining a traveller during their journey is comparatively much simpler, due to their physical presence at the time. Furthermore, for airlines, valuable time and effort would be required, which can be better spent trying to detect and stop travel that has not yet flown. However, work is progressing to identify prolific travellers, who travel many hundreds of times on illegitimate tickets, by both law enforcement, and the travel industry. One of the biggest issues with policing travel fraud may be taking action against those responsible for making the fraudulent bookings, rather than the travellers.

There were indications that efforts to involve law enforcement were improving. Participants credited Europol and the National Cyber-Forensics and Training Alliance for helping to address this issue. Some law enforcement agencies had also started to recognize the problem, with the Greek cybercrime unit opening a reporting platform to receive incidents from the travel industry.

Of course, the problem is not solely about getting law enforcement involved. A related concern is the travel industry not reporting this type of fraud to the police. Due to the volume of fraud identified, and many bookings being made at the last minute, the most common response was to cancel the ticket, without any reporting. It was also believed that the time and resources required to cooperate with a police investigation would be too extensive and expensive to be of value. In some countries, trust in law enforcement may be lacking, hindering cooperation with the travel industry.

Conclusion and discussion

This research found that sellers of fraudulently obtained airline tickets operating on anonymous online blackmarkets are also selling other goods and services. These include other travel services, such as hotel accommodation and car hire, as well as compromised data, services to enable fraud, and drugs. Some sellers have also attempted to purchase compromised data. Buyers are also purchasing fraud enabling services and stolen credentials. Those purchasing travel on these marketplaces often state that they were doing so for ‘clients’, indicating that they were providing tickets to others, whether they were victim travellers, mules, or others.

While there was some evidence of trade in other goods and services by buyers and sellers, there is a limitation in the data examined for this research. As the data only relates to travel fraud, it does not capture the same buyers and sellers posting on other threads, and the data relates to just one forum, while the actors may operate across different marketplaces. There is scope for additional work to identify what other related goods and services buyers and sellers are trading in on the anonymous online blackmarkets.

The chatter on the marketplaces indicates that there is demand for cheap tickets. Sellers also claim that they are processing large numbers of orders, although this may be an exaggeration to make their shopfront appear attractive. The number of travellers stopped during the global action days (1,219 during the years 2013–18), and the number of bookings cancelled before travel also indicate that the market is not insignificant. The number of travellers detained during global action days regularly exceeds 100, and this is only for tickets purchased using compromised card data, rather than other methods.

The extent of trade was not measured quantitatively in this research, and understanding the true extent can be problematic. Potential ways that can be explored further include the amount of trade that a seller is involved in, the size of the market on the various forums, the number of chargebacks, and the cost to the provider. It may be possible to verify the amount of trade by sellers through escrow transactions, Bitcoin payments or feedback. Analyses such as that performed by Soska and Christin (2015) (which primarily related to the drug trade), could provide an estimate of the overall trade in travel services on the marketplaces, by volume of sales and number of sellers, over time.

Participants mainly spoke about the retail ticket price when it came to the financial impact on the airline. This can be thought of as the opportunity cost, with the alternative being the traveller legitimately purchasing a ticket. Another way to conceptualize costs would be the actual financial cost to the airline, such as fuel to carry the extra weight, as well as catering and other service costs incurred. This may vary if the flight is fully booked, as a fraudulent ticket may result in the loss of a legitimate booking by another traveller. The absence of a method to enable airlines to discover the actual cost to them of fraud hampers investment in doing something about it.

Travel fraud is a global crime. Some of the regions that were identified in this study were due to the participants spoken to (for example, the regions serviced by specific airlines). Other routes are identified as having more detected fraud than others, and in some cases, it was believed that this was linked to certain crime types, such as smuggling drugs, human trafficking, and human smuggling. Some of the destinations peak seasonally, or during world events.

Travel fraud has changed over time. This change has been driven by new opportunities, as well as displacement, as old methods have become more difficult to carry out successfully. This explains why there are so many different methods through which tickets can be fraudulently obtained. It is likely that offenders will continue to innovate, taking advantage of different ways the travel industry serves their legitimate customers, as well as new, and existing, fraud methods that arise. One example of this is the role that Bitcoin may take in the travel fraud business, particularly as airlines begin offering this as a payment method. Questions were raised about future Bitcoin payments, as there is no chargeback mechanism, and therefore no incentive to detect fraudulent transactions. Furthermore, the role that insiders have in the travel fraud economy may become more apparent as the industry starts to take this threat more seriously.

Law enforcement may be reluctant to pursue travel fraud cases due to their transnational nature, which makes it difficult to obtain evidence and prolongs the investigation. Some of the additional challenges for law enforcement relate to understanding the travel fraud problem. The use of proforma interview schedules, to ask detailed and pertinent questions and seek evidence, may be beneficial. Feeding the intelligence gained back to an international system would also be advantageous, so that it can be reviewed strategically. Ultimately, focusing on those obtaining the tickets, rather than the travellers, may have more impact. Law enforcement can also learn from their international counterparts who are starting to provide central points of contact for receiving reports of fraud from the travel industry.

This research has attempted to overcome the significant difficulties associated with this challenging area of research. However, a number of limitations in the research design are identified. First, while participants were from the USA, Asia, and Europe, there may be regional differences that have not been identified. Second, the sample size and way that participants were referred may introduce bias into the results. And finally, as this research is exploratory, it is not attempted to quantify the various aspects that have been identified.

Funding

This work was supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS\&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131] (to 30 September 2016); and the UK Engineering and Physical Sciences Research Council (EPSRC) [grant EP/M020320/1] for the University of Cambridge, Cambridge Cybercrime Centre (from 1 October 2016). The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

Acknowledgements

I thank and acknowledge all participants who agreed to be formally interviewed, or who met with me informally for the purpose of this research. All participants were passionate and enthusiastic about their work, which often was in very challenging environments with competing priorities. Many came with a vast amount of experience, and had made considerable inroads in trying to combat travel fraud. The analyst who assisted with facilitating interviews, a visit, and access to case material deserves a special thank you for their efforts. Finally, this work would also not have been possible without the valuable assistance of Nicolas Christin and Kyle Soska at Carnegie Mellon University, Richard Clayton and Ross Anderson at the University of Cambridge, and my other colleagues in the Cambridge Cybercrime Centre.

References

Boggan, S. (2006). ‘What could a boarding pass tell an identity fraudster about you? Way too much’. Available online at: https://www.theguardian.com/business/2006/may/03/theairlineindustry.idcards.

Broséus, J., Rhumorbarbe, D., Mireault, C. *et al.* (2016). ‘Studying Illicit Drug Trafficking on Darknet Markets: Structure and Organisation from a Canadian Perspective’. *Forensic Science International* **264**: 7–14.

Christin, N. (2013). *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace, 22nd International Conference on World Wide Web*, Rio de Janeiro.

Crime and Justice. (2014). ‘Ilford phishing fraudsters jailed’. Available online at: http://crimeandjustice.co.uk/2014/07/17/ilford-phishing-fraudsters-jailed/.

Europol. (2013). ‘European day of action targets airline fraudsters’. Available online at: https://www.europol.europa.eu/newsroom/news/european-day-of-action-targets-airline-fraudsters.

Europol. (2014a). ‘113 people detained and 70 arrested in action day tackling airline fraud’. Available online at: https://www.europol.europa.eu/newsroom/news/113-people-detained-and-70-arrested-in-action-day-tackling-airline-fraud.

Europol. (2014b). ‘118 arrested in global action against online fraudsters in the airline sector’. Available online at: https://www.europol.europa.eu/newsroom/news/118-arrested-in-global-action-against-online-fraudsters-in-airline-sector.

Europol. (2015a). ‘133 people detained in global action tackling airline fraud’. Available online at: https://www.europol.europa.eu/newsroom/news/133-people-detained-in-global-action-tackling-airline-fraud.

Europol. (2015b). ‘Fake online travel agency selling plane tickets dismantled’. Available online at: https://www.europol.europa.eu/newsroom/news/fake-online-travel-agency-selling-plane-tickets-dismantled.

Europol. (2015c). ‘Global action against online air ticket fraudsters sees 130 detained’. Available online at: https://www.europol.europa.eu/content/global-action-against-online-air-ticket-fraudsters-sees-130-detained

Europol. (2016). ‘Global action against airline fraudsters: 193 detained’. Available online at: https://www.europol.europa.eu/newsroom/news/global-action-against-airline-fraudsters-193-detained.

Europol. (2017a). ‘153 detained for ticket fraud following worldwide law enforcement operation’. Available online at: https://www.europol.europa.eu/newsroom/news/153-detained-for-ticket-fraud-following-worldwide-law-enforcement-operation.

Europol. (2017b). ‘195 individuals detained as a result of global crackdown on airline ticket fraud’. Available online at: https://www.europol.europa.eu/newsroom/news/195-individuals-detained-result-of-global-crackdown-airline-ticket-fraud.

Europol. (2018). ‘141 arrested in worldwide crackdown on airline fraud’. Available online at: https://www.europol.europa.eu/newsroom/news/141-arrested-in-worldwide-crackdown-airline-fraud.

Felson, M. (1994). *Crime and Everyday Life.* Thousand Oakes: Pine Forge Press.

Gibbs, G. (2007). *Analyzing Qualitative Data.* London: SAGE Publications Ltd.

Hasbrouck, E. (2001). *The Practical Nomad Guide to the Online Travel Marketplace.* Emeryville: Avalon Travel.

Holt, T. J. (2013). ‘Exploring the social organisation and structure of stolen data markets’. *Global Crime* **14**(2–3): 155–174.

Holt, T. J. and Lampke, E. (2010). ‘Exploring Stolen Data Markets Online: Products and Market Forces’. *Criminal Justice Studies: A Critical Journal of Crime, Law and Society* **23**(1): 33–50.

Holt, T. J., Smirnova, O., and Hutchings, A. (2016). ‘Examining Signals of Trust in Criminal Markets Online’. *Journal of Cybersecurity* **2**(2): 137–145.

Hutchings, A. (2014). ‘Crime from the Keyboard: Organised Cybercrime, Co-Offending, Initiation and Knowledge Transmission’. *Crime Law & Social Change* **62**(1): 1–20.

Hutchings, A. (2018). ‘Leaving on a Jet Plane: The Trade in Fraudulently Obtained Airline Tickets’. *Crime, Law & Social Change* 1–27.

Hutchings, A. and Holt, T. J. (2015). ‘A Crime Script Analysis of the Online Stolen Data Market’. *British Journal of Criminology* **55**(3): 596–614.

Jaroszewski, P. (2016). *How to Get Good Seats in the Security Theatre? Hacking Boarding Passes for Fun and Profit.* Las Vegas: Defcon.

Krebs, B. (2012). ‘Donkey express: Mules take over the mail’. Available online at: https://krebsonsecurity.com/tag/reshipping-scams.

Meiklejohn, S. and Mercer, R. (2018). ‘Möbius: Trustless Tumbling for Transaction Privacy’. *Proceedings on Privacy Enhancing Technologies* **2018**(2): 105–121.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G. M. (2011). *An Analysis of Underground Forums, ACM SIGCOMM Conference on Internet Measurement*, Berlin.

Nohl, K. (2016). *Where in the World Is Carmen Sandiego?, Chaos Communication Congress*, Hamburg.

Smith, R. G., Wolanin, N., and Worthington, G. (2003). *e-Crime Solutions and Crime Displacement. Trends & Issues in Crime and Criminal Justice No. 243*. Canberra: Australian Institute of Criminology.

Soska, K. and Christin, N. (2015). *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, 24th USENIX Security Symposium*, Washington, DC.

Tajalizadehkhoob, S., Asghari, H., Gañán, C., and van Eeten, M. (2014). *Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware, Workshop on the Economics of Information Security*, State College.

The United States Department of Justice (2017). 'West African Computer Hacker Sentenced to Federal Prison.' Available online at: https://www.justice.gov/usao-ndga/pr/west-african-computer-hacker-sentenced-federal-prison.