Trends Organ Crim (2012) 15:111–129
DOI 10.1007/s12117-012-9159-z

Cybercrime and virtual offender convergence settings

Melvin R. J. Soudijn · Birgit C. H. T Zegers

Published online: 25 May 2012

Abstract Felson coined the term 'offender convergence settings' to describe certain physical locations, e.g. local tough bars, in which (potential) offenders meet each other. Here they relax with friends and acquaintances, meet new people, exchange information, sell stolen material or plan new criminal acts. The perpetrators of cybercrime also make use of such locations, albeit digitally in so-called virtual forums. From a law enforcement point of view, both types of settings should be suppressed. However, a physical location is easier closed down than a virtual one. This is because the virtual forum is often situated in countries that will not cooperate with requests to take down servers. This could be considered as an advantage for the offender. But virtual forums also have specific disadvantages. Every contact and discussion is digitally preserved for those who know where to look. A law enforcement agency was able to take such a look in one particular forum. This revealed over 150,000 postings by 1,846 members. More importantly, these postings disclosed crime scripts as criminals themselves see it. It turns out that hacking accounts and stealing money is not their biggest problem. What is a risk, however, is not leaving traces when wiring the money into other accounts. This article tries to translate such insights in policy recommendations.

Keywords Cybercrime · Carding · Situational crime prevention · Offender convergence setting

The authors would like to thank F. van der Laan (Slavist, researcher and deputy teamleader Strategic Analysis Dutch National Crime Squad), E. Monsma (researcher Team High Tech Crime at the Dutch National Crime Squad) and P. Takkenberg (teamleader Team High Tech Crime at the Dutch National Crime Squad) for their comments

The views expressed are personal and in no way represent those of the Netherlands Police Agency.

M. R. J. Soudijn (✉) · B. C. H. T. Zegers
National Crime Squad of the Netherlands Police Agency,
P.O. Box 100, 3970 AC Driebergen, The Netherlands
e-mail: Melvin.soudijn@klpd.politie.nl

Introduction

Would you respond to an advertisement for earning easy money? When the only thing you have to do is to withdraw money in cash that is paid into your bank account and then send the money by means of money transfers to people in Russia? You are allowed to keep 5 % of the money to be transferred for yourself…

It is most likely that readers of this article will suspect a catch. In 2008 however, fifteen people in the Netherlands responded positively to such an advertisement. Alas, if money can be earned so easily, then it is often too good to be true, as was the case here. The money apparently came from digital fraud concerning payment orders. Although the fifteen people were not responsible for setting up this fraud, they did however make it possible for the money, which was fraudulently come by, to disappear from view. When the bank in question that was being defrauded discovered what was going on, they reported it to the police in the Netherlands. It did not take long to trace the fifteen Dutch people, since they had used their own bank accounts. However, the money had already been sent on to their Russian commissioning parties. The Dutch authorities then contacted the Russian authorities concerning those commissioning parties. This collaboration finally resulted in the arrest of a few of these people. It transpired that these offenders were involved in the so-called 'carding' scene.

Carding is a term used in the world of cybercrime and involves the fraudulent use of personal data taken from bank cards and credit cards (Peretti 2008). With the increase in the use of the internet for payment orders, a new criminal market has also been created, namely the illegal trade in financial and/or private data with which unauthorized transactions or payments can be carried out. In a survey carried out by the Central Bureau of Statistics in the Netherlands of 4,000 Dutch internet users, 1 % of the respondents had suffered loss through fraudulent use of guaranteed cheques and 2 % had suffered financial loss through 'phishing' (CBS 2010). The Netherlands Bankers' Association publicly acknowledges that internet banking fraud is a rapidly rising cost item. In 2010 the loss was estimated at EUR 9.8 million, compared with EUR 1.9 million in 2009.[1]

Research has shown that carders (people involved in carding) can find each other through specialized online carding forums (Holt and Lampke 2009; Peretti 2008). Some of these carding forums are open to anyone who is interested in this type of illegal activity, whilst other forums have protected entry. These carding forums have a number of different functions; they provide a meeting place where carders can exchange information, start new illicit processes or deal in stolen data, goods, services and software.

In this way, the forums display strong similarities to what Felson calls "offender convergence settings" (Felson 2003). He is referring to physical locations where offenders converge and which then become central to crime. Offenders congregate at such places for relaxation, to exchange information, to buy and sell stolen goods, etc. These activities can take place, for example, in restaurants that are in the hands of organized crime figures. Abadinsky called these "the right spots": places where professional criminals can meet each other (Abadinsky 1983, p. 29). At a different level, these spots might be represented by the local fast food outlet or an empty school

[1] http://www.veiligbankieren.nl/nl/nieuws/14-03-2011_intensieve-samenwerking-politie_justitie-en-banken-tegen-internetfraude.html

playground where young people hang around together in the evenings. A physical place, however, is not always required. It has already been shown that pedophiles meet each other in certain online networks (Trembley 2006). Since carding forums only exist in cyberspace, in this case one might talk of *virtual* offender convergence settings.

One such virtual offender convergence setting came to light during the Dutch police investigations. Although the forum had blocked entry to unidentified visitors, a technical fault caused a leak in 2008. This provided the High Tech Crime (HTC) team of the Netherlands Police Agency with the opportunity to make a digital copy of the forum, which provided the police an extraordinary perspective on the matter of carding. On the basis of the communication between the members of the forum, they were able to gain insight into all the ins and outs that the crime of carding involved. As such, the offenders themselves gave an indication of their crime script. This raises the question as to whether such a script could also provide insight into the moments at which criminals are vulnerable. Identifying such vulnerabilities can provide the opportunity for policy makers and investigating authorities to influence the situation to their own advantage. But where are those opportunities? Which measures can be formulated in the area of situational crime prevention through analysis of the carding forum?

In order to answer these questions, this article is organized as follows. In the section 'Data and method', further details will be given concerning the forum that was intercepted by the Dutch police and the method of analysis. The membership, the organization, the type of messages and the mutual communications will be discussed. Following on, in section three, a crime script will be described as it emerged from communications on the forum. We differentiate between four phases, those being the preparatory phase, the theft of data, the deployment of so-called money mules and the payout of the criminal profits. On the basis of this crime script, the main research question will be answered in section four. At the end of the article, in the 'concluding remarks', there is discussion about combating carding and theoretical implications of offender convergence settings.

Data and method

To give the reader a general idea about the kind of information that could be found on the forum, it is necessary to explain the structure and dynamics of the forum in more detail.

The forum was set up in the spring of 2003. There were 1,846 members in total who took part in the forum. At no point were they required to register their true identity and they were only known by their nicknames.[2] Because the HTC team was able to make a digital copy in 2008, the police were able to retrieve all postings that had been made up to that time. This amounted to 153,936 postings and 60,437 private messages. Data from the forum thereby represents a sizeable reference document in the area of carding and all that goes with it.

The forum served two general functions: a place for exchanging knowledge and a place where people either offering or in search of products and services could meet each other. The knowledge transfer function and the market place function took place through the placement of messages, questions and offers to which members were able to react.

[2] The 1,846 members should not be taken to be the same number of natural persons. It is perfectly possible for one person to be logged in under multiple identities.

Sections were set out for the exchange of knowledge and for deals, so that members could determine where they could go for what they needed and where they could find the services they needed in the area of carding. For example, under the section 'real carding', a long discussion was carried out about how a person could take out money from a cash dispenser without being recognized by the security camera. There were also discussions concerning the choice of cash dispenser where skim apparatus could be installed.[3] The advice included that choices should take into account towns with more than 15,000 inhabitants, places which attract a lot of tourists, places where not too many people come and go during the morning rush hour, and places where there is no bar in the vicinity where people hang around outside. Through this sort of advice it has been possible to gain a good insight into the carding script in the way that the offenders themselves experience it.

Not only were discussions carried out and advice given on the forum, but it was also a place where the various market parties could also come into contact with each other. Some were dealing in stolen credit cards, others were available to be hired in to accept money transfers, yet others could be deployed in graphic design for creating fake websites, and another group could act as intermediary in the rental of an anonymous server, etc.

The actual business deal could not, however, take place on the forum because that was against the forum rules. This was in the hope that the investigating authorities would find fewer leads for prosecution and thereby give the matter less priority. To make business agreements the members had to use different communication systems instead, such as messaging via ICQ numbers. This results in a limitation in the research data. The forum certainly provides insight into the type of goods or activities that are offered, but not in the business discussions between the members and how often actual transactions in goods and/or services took place.

Besides all sorts of security measures used against investigating authorities, the forum also did its best to attract clientele that were as trustworthy as possible through a system of giving guarantees, peer review and status. This worked in the following way: in order to become a member of the forum a person had to pay the sum of USD 50. This would enable setting up a user name and password. Those people who wished to have full access to all the messages would have to find two forum members who were willing to stand as guarantors.

Peer review was created by the members awarding marks to each other's goods and services. That mark gave an indication of how trustworthy a person was with whom to do business. Just like on eBay, a person with plenty of positive reviews will appear more trustworthy than someone who is just starting out and has no feedback yet.

The forum members were also given a status. This gave an indication about the trustworthiness too, as well as the rights that the person held in the forum. The following statuses were awarded by the forum members:

- The status of Moderator is kept for those people who can award a status to other people or disallow it again.

[3] Using this apparatus makes it possible to copy credit card data from ATMs in public places or POS terminals in shops.

- The status Newcomer is awarded to someone after registration in the forum, but without any guarantees from other forum members. The Newcomer does not have access to all the available information.
- The status Member is awarded to someone if two people are willing to act as their guarantors. This leads to access to the whole forum.
- The status Service denotes that the person in question is permitted to sell their goods or services. In order to achieve this status, the administrator of the forum will need to be paid.
- The status Verified Member is awarded to people who are trusted by the forum because they have been checked out by the moderators.
- The status Administrator. Administrators are responsible for checking the content of postings and placing postings in the correct sub forums.
- The status Deer is awarded to someone who has broken the forum's rules.
- The status Unresolved Problems is awarded to someone with whom another forum member has a business problem that has not yet been resolved.
- The status Ripper is given to a person who has cheated on another forum member.[4]

It can be seen from this summary that a person's status could change over the course of time. A person could achieve a higher position by paying more, finding guarantors and by being trusted by the moderators. However, a person could also lose status. There are at least three negative statuses described. They vary from someone who has broken the forum rules through to someone who is guilty of cheating other forum members.

Although the system of standing guarantee, peer review and status served to give as transparent a picture as possible of their business partners, this transparency had to be taken with a pinch of salt. The identity of the members remained undisclosed because everyone participating in the forum used only nicknames. Moreover a negative status could also be reversed through the payment of fines and by finding new guarantors.

All in all, the total amount of information contained within this forum is quite enormous. Earlier research already carried out quantitative analysis on this forum. With the use of statistical techniques and Social Network Analysis, the forum was evaluated in terms of centrality. Logistic regression with two-way clustering was used to test the hypothesized effects of individual characteristics on network centrality. The results showed that there was considerable variation in centrality. The network didn't have a typical core-periphery structure. Central network positions were not scarce but cooperation seemed to be self organized without central direction.

Such findings, however, don't answer our basic research question on the possibility of the use of situational crime prevention techniques. Or to put the matter differently, the quantitative findings only makes it more necessary that such techniques are developed. When there are no kingpins or essential nodes in the forum, the usual police response of searching for and taking out individual crime bosses becomes an ineffective strategy in the long run. When no one is indispensable, any criminal taken off the board is easily replaced. In contrast, situational crime

[4] As opposed to ripping in the everyday drugs market, in this context ripping incurs no physical repercussions. The only reprisal used against negative feedback is ostracism.

prevention theory is about removing the opportunities for sustaining the forms of organization and networks that are necessary to commit certain crimes (Bullock et al. 2010).

In finding alternative strategies to combat carding, a qualitative analysis of the forum is therefore suited. In this article we used a form of textual analysis, not counting the frequency of certain keywords but focusing instead on what was being communicated. This enabled us to construct an ideal crime script. Although different crime scripts could be built depending on the sort of stolen financial information or the payout, we focused on a crime script that related to the incident in the Netherlands that was described in the introduction. Because the number of postings and messages on the forum is enormous, we cherry picked the ones that held (in our view) the most interesting information on this particular form of carding, i.e. background discussions, extensive explanations of carding problems, comments on failed or succeeded projects etc. Of course, there is always the possibility that we discarded some postings as irrelevant or overlooked other information that with hindsight could be used to construct preventative measures. However, the crime script described in this article was practical and can always be fine tuned in the future.

Carding process

The ultimate aim of carding is to make financial gains through stolen financial data. These financial gains can be brought about in several different ways. Peretti (2008) distinguishes four forms, namely carding online (purchasing goods online with stolen credit card information), in-store carding (presenting a counterfeit credit card, which has been encoded with stolen account information, to a cashier at a physical retail store location), gift card vending (purchasing gift cards and reselling them at a discount) and cashing (obtaining money instead of goods with the stolen financial information).

Separate crime scripts can be written for each and every carding variety. However, this article will only deal with the cashing form because that is what the Dutch investigation encountered (see introduction). Otherwise, this article would exceed size restrictions.

The textual analysis of the forum showed that the cashing process can be roughly divided into four phases. These entail the preparatory phase, the theft phase in which the credit card or other bank data is stolen, a money mule phase in which the money is transferred and finally the cashing phase, the phase in which the fraudulently received money arrives in the hands of the main suspect(s).

The preparatory phase

During this phase the carder makes a plan of attack for a cashing project. Depending on the level of control that the carder wishes to maintain over the whole process, a number of other partners will be approached in the forum. These partners will be recognized specialists in particular areas where the carder is less knowledgeable, has less time for or less interest in. These specialties will be researched extensively during the following phase.

Once the contacts have been made with the future business partners, an infrastructure is set up that allows the carder and partners to store information anonymously and exchange and process information with each other. Therefore it is important to protect this infrastructure very carefully from investigating authorities (and competitors). The offenders are quite obviously aware of the difficulties that the authorities experience when it comes to international crime.

A member of the forum listed all the countries that have signed the Convention for Cybercrime and consequently where active judicial collaboration can be expected. Someone advised using servers in China and Hong Kong, even though this often leads to slow connections. Malaysia and Panama offshore are better. A company was established thereby, one specialized in such exotic connections. Someone else suggested the Netherlands as a safe country. Not everyone agreed with that. Another person suggested the combination of the Netherlands with Switzerland or vice versa.

Source: HTC interception

The partners do not meet each other in the flesh, but they keep digital appointments. The mutual settlements are also made digitally. One method used for doing this is the WebMoney system, a digital payment system whereby use is made of electronic money. However, preferences can change in this area. For instance, in 2003 there were heated discussions on the forum about the advantages and disadvantages of WebMoney. It was not clear then to everyone what advantages were actually offered by the system. Doubts were raised as to whether you could use WebMoney for worldwide payments. But by 2008 the use of WebMoney was accepted throughout the forum. The reason for this is that cybercriminals had found out in the meantime how to transfer money from a WebMoney account to bank cards that can be used for withdrawing cash from a cash dispenser.

The theft

Cashing can only take place if financial data has been stolen concerning credit cards or other bank data. The theft of this data can take place in various ways. These can be divided up roughly into four methods, namely skimming, hacking, receiving stolen property, and phishing (KLPD/DNR 2010).

1. In the case of skimming, the data is taken directly from the card by manipulating the card readers at ATMs and POS terminals. In some cases it appears that a shop assistant or waiter/waitress makes an extra copy of the magnetic strip when processing a payment by card in order to sell this on at a later time.
2. In case of hacking, a cybercriminal steals the files containing the credit card data, for example, of clients of internet shops. All sorts of digital methods are used to break into the shop in order to steal the data.
3. In case of receiving stolen goods, an employee steals client data from their employer and then sells this on.
4. In case of phishing, the cybercriminal breaks into the computers of unsuspecting consumers with the help of malware (malicious software). This provides the criminal with access to the computer, which then makes it possible to see what the victim is doing. At the moment when the victim starts an online banking session,

the cybercriminal breaks into the session without the victim being aware of this. The banking session is then taken over by the cybercriminal and manipulated by placing transactions 'ready', which the victim then authorizes unwittingly.

In other words, the theft phase can be carried out in several different ways. In the case cited in the Netherlands, a phishing method was used. The carder had sent an e-mail to clients of a specific bank that would cause the computer of the bank client to become infected. The e-mail appeared to come from the bank itself and requested the unsuspecting client to click on an internet link. By clicking on this link, malware would be downloaded onto the victim's computer.

There is a wide range of malware for sale on the forum. There is an advertisement, for example, for 'Limbo 2 Universal Grabber'. This is a package of malicious software, which installs itself on an infected computer and which has various functions. A seller on the forum described it as follows:

This type of 'malware' is capable of registering all the websites where the user logs in as well as the keyboard strikes deployed by the user when signing into an e-mail address. The malware is not detected by antivirus software and if it is, then the malware will be updated so that this can be reinstalled and remain undetected. Payment for such a package must be made via a WebMoney account.

Source: HTC interception

It is likely that the carder will have collaborated with various different partners during the theft phase. For example, the e-mail that was sent out to the clients of a particular bank was written in Dutch. It is likely that is was translated into Dutch by a translator, since a message without language errors has a greater chance of fooling the victims. This costs money, however, all the more to pay for the certainty that translators will not report the action to the police. A forum member provided the following service:

Translation and composition of texts, corrected by native speakers, in every common language. USD 25 per 100 words of original text. Copywriting: USD 50 per 100 words.

Source: HTC interception

Money mules

In the case in the Netherlands, the theft involved data with which fraudulent bank orders for transfers were generated. However, there is little point in fraudulently transferring money to another bank account if the digital trail left by the money cannot be concealed. Otherwise the offenders would be presented more or less on a plate to the investigating authorities. Moreover, the direct transfer of money to a bank account in Russia or the Ukraine (where most carders appeared to live) could arouse suspicion by the banks in question, which could react by blocking accounts.

In order to avoid such problems the carders use so-called money mules or drops. [5] These are people who, in exchange for a small payment, make their own

[5] Drops are people who can receive both money and goods. The term money mule is used consistently in this article because of the focus on money flows.

bank account available for money transfers. The money must then be withdrawn in cash (thus breaking the digital trail) in order to then be transferred to the commissioning party by a different method (e.g. Western Union).

The term money mule is a fitting description of such a person who only carries money back and forth. They can only be used for a short period, because once a digital fraud has been discovered they can quickly be traced (as in the case in the Netherlands). Of course, the money mules are not told this. Instead they are given job titles such as Financial Department Manager. The following text shows an example of an e-mail used in recruiting money mules:

Hello!,

My name is VLADIMIR TOPALOV, I'm a HR MANAGER of the MIMOTRANS payment system financial department, which enters MIMO Finance group.

Due to our company amendment in the Europe market we need a new staff. And now we are glad to offer you a vacant position of Financial Department Manager of our company.

We can offer you:

-high regular income

-career development potential

-14-days paid vacation

-work in a friendly team

-bonuses and loyalty program for the company employees

-and other

You can get all of that working with us without leaving your home as the job which we are glad to offer you, requires spending of just a few hours per day near your computer.

Your minimal income is $2,000 per month. You are getting 5 % of each money transfer. Moreover we pay all expenditures and system commissions.

Source: HTC interception

In the case in the Netherlands, the carder was looking for a partner that could manage the whole of the money mule process. This is a labour intensive process. For example, the money mules must be recruited by sending out plausible e-mails after which contact is made with those people who react to these e-mails; they then need to be given instructions for every transaction required in transferring the money. This makes the money mule service a costly business for the carder. The tariffs can be as much as 50 % of the amount to be transferred.

In the case in the Netherlands, the money mules were provided with written instructions stating exactly how they should go about the task:

You receive the money from our clients, after which you go to your bank and withdraw the money in cash from your bank account. You then go to Western Union bank or Money Gram where you transfer 90 % via the above-mentioned bank systems. The details will be given to you by our operator, together with the assignment. Withdrawing the money from your bank account and then transferring the money should take no longer than 2 h. When the 2 h have passed, you must return home and send a message to our firm in which you report the details of the money transaction.

Source: HTC interception

The moment when the money was deposited into the money mule's bank account, the money mule would receive the following message.

Congratulations with the start of the work for our company. Today a client of our company has sent money to your bank account.

Source: HTC interception

In other cases, however, instructions could be given over the telephone. Various forum members also offer professional telephone services for this reason.

A provider has men's and women's voices available that can make telephone calls at night from Moscow (during American office hours) in English or German. The telephone calls cost USD 10 each. A 24 h service is also available on request. The business is specialized in calls concerning banks, payment systems, casinos, shops, dating and eBay.

Source: HTC interception

Coordination of the money mules is extremely important because withdrawals carried out haphazardly by money mules could lead to the whole fraud being uncovered, after which the banks would still be able to block the money.

There was also discussion on the forum about which method was the best for transferring money. The following example is a discussion about SWIFT, the identification code used by banks for international money flows, and Western Union, a worldwide network of offices where money transfers can be carried out. Or as one forum member stated:

SWIFT is solid, on the one hand it's reliable in the sense that you know that your money will arrive in the right place, but on the other hand Money Transfers are viewed with suspicion by investigating agencies. The money gets there quicker via Western Union than via SWIFT. Still, the advantage with SWIFT is that reverse transactions or error reports generally take longer than it takes for the receiver to withdraw the money from the account. (forum)

Source: HTC interception

A coordinator will try to follow the complete transfer process by being able to monitor the money mule's bank accounts. Sometimes a coordinator will keep a specially designed bookkeeping system in which the whole procedure can be accurately recorded: when the money is deposited into the money mule's account, when the money mule should withdraw the money, when the money mule should forward the money, as well as all the relevant amounts.

The cashing phase

The money should reach the hands of the carder during this phase. This is still a risk for the carder because the withdrawal of money can form a link in the criminal money trail. There was a discussion on the forum about what might be a safe way for

someone to withdraw large sums of money from cash dispensers. People are not only afraid of being caught, but the machines themselves sometimes present a problem. Either they simply do not work or they have limits whereby all of the money cannot be withdrawn within one day. A member of the forum therefore posted a number of guidelines concerning the illegal withdrawal of money from ATM machines.

Gentlemen, let's just make a list of the things that mainly concern that which we need to keep a lookout for:

1. Cameras that are placed by ATMs (*you are advised to wear jumpers, baseball shirts, shawls, hoods, in other words anything with which you can partly cover your face. Watches, unusual rings and tattoos must be kept covered up*).
2. People in uniform who could approach you (*The best idea is to have someone else nearby who can give a warning if necessary*).
3. Being traced nearby the cash withdrawal (*take care that you are not recorded by any other camera in the neighbourhood of the ATM*).
4. Ambush (*these are usually set up at places where there are 3 or 4 ATMs close together. Best to avoid such points)*.
5. Security in the shop next to the ATM (*don't draw attention to yourself)*.

Source: HTC interception

In order to limit the risks to themselves, carders can also employ a specialized service provider at this point, who will make the money withdrawals instead. One example on the forum is a person who offers cash withdrawals from Western Union and Money Gram in the Ukraine.

The minimum amount that can be cashed is USD 100, with a commission of 7 %. The limit is 10,000 per person per day. Working hours are from 10 a.m. to 8 p.m. on Monday to Friday, and from 10 a.m. to 4 p.m. on Saturday and Sunday.

Source: HTC interception

The cash withdrawals were not made by the advertiser himself. He indicated that he coordinated the withdrawals by directing other people. The people who made the cash withdrawals would hand over the money to the coordinator who would in turn contact the carder. Anonymity could be maintained during this last phase by depositing the cash in a deposit box in a public place, for example. There is no information about this stage in the case in the Netherlands.

Situational crime prevention

A number of measures will be put forward in the following two sections to prevent carding in general and cashing in particular. The measures are aimed on the one hand at the offender convergence setting with the aim of disrupting the market. On the other hand some thoughts are given to specific measures that will disrupt the crime script for cashing. These measures are mainly theoretical, but there are a few cases where they have been tried out in practice.

Offender convergence settings

The previous sections have made it clear that dozens of people can be involved in setting up fraud via cashing. Particularly in the case of large-scale cashing projects the fraud is divided into different activities, each being carried out by different people. These vary from providing malware, collecting credit card data, sending fraudulent bank payment orders, setting up and coordinating a network of money mules to receive the money, a translation service, right through to a network of people willing to withdraw cash from ATMs. As we have seen in the previous sections, each of these activities need specific skills. The people offering such skills will look for each other in a few specific carding forums in order to exchange information and to take on new criminal projects. This essentially means the forums function as virtual offender convergence settings.

These virtual aspects of forums resulted in a few special characteristics. First and foremost is the fact that there is no physical contact. People get to know each other using nicknames via e-mail and they seldom have face-to-face meetings. The lack of physical contact also leads to a different type of 'discipline' in case of undesirable behavior (ripping). Conflicts are not fought out using violence and firearms, but by giving each other bad reviews. The forums are also not affected by closing times nor influenced by weather conditions. The forums are online and therefore available 24 h a day. By simply remaining logged in, a person can be present the whole day long. Commuting to and from a forum presents no problems. Moreover, the forums can be accessed from any given location thanks to mobile connections via smartphones or laptops, for example. The meeting place is also sizeable: where a cafe can only offer enough space for a limited number of people, forums can provide room for hundreds of active members at any one time. All these differences add up to making the mutual interaction even stronger.

The concept of offender convergence settings is based on the idea that such settings facilitate co-offending. Co-offending means that at least one crime and two or more offenders are involved. That involvement can be in the preparatory dealings, the principal offence or other support. In case of the latter, take for example a burglar who steals goods and afterwards takes the stolen goods to a fence. This is co-offending in money laundering.

Offender convergence settings facilitate co-offending because they offer a specific location where like-minded people can meet each other. Since offenders relax together in such settings, they get to know each other better and a form of trust is built up. Felson calls this a mutual discovery process (Felson 2003, p. 159). That trust makes it easier to find trustworthy co-offenders at a later date, which in turn leads to the creation of a broad network of criminal contacts.

Probably the most important theoretical insight that arises from the reasoning concerning offender convergence settings is that the locations provide "structure and continuity in the face of individual, group, or network instabilities" (Felson 2003, p. 158). That insight adds weight to the idea that criminal collaboration takes place in the form of dyadic relationships within networks (Coles 2001; Heber 2009; Morselli and Giguere 2006; Southerland and Potter 1993; Zaitch 2002; Zhang and Chin 2003). It is known that the membership of networks is fluid, particularly when the participants themselves are unstable. By shifting the focus from networks to fixed locations, this appears to involve an "accomplice regeneration process" (Felson 2003,

p. 160). This means that new offenders join in, offenders who have no manifest or latent ties with existing criminals. When new offenders start to frequent the existing criminogenic settings, then potential connections are made for new sets of co-offenders (von Lampe 2009). Therefore criminogenic settings help to explain the creation of new forms of criminal collaboration (Felson 2003, 2006).

The existence of offender convergence settings therefore holds various advantages for criminals. They provide a situation that is good for diverse forms of contact, where you can pick up tidbits of information and where deals can be struck.

However, there are also potential risks involved. It is more or less unimaginable that the police would not know about such settings (through community policing, for example). Scientific analysis of self-reporting studies, for example, can also determine such settings (Bichler & Malm and Enriquez J 2011). Knowledge of such a criminogenic setting is therefore almost bound to summon some form of reaction from the authorities. For example, the police can send undercover agents to the offender convergence settings to gather information. Or a local council can decide to close down a location that is causing too much public nuisance and other problems. In other words, "eliminating" offender settings can impair gangs' abilities (Ayling 2009).

As well as the physical meeting places, virtual meeting places also run risks. Investigating units specialized in computer crime are able to bring such forums into view. Since carding forums evidently support criminal activities, the obvious answer is to ban them completely. Moreover, because the forums have no physical presence in a local community, the closure would not be at odds with the policies of local interest groups.

However, the elimination of carding forums is not such a simple task. In practice, disabling a server infrastructure (on which the forums are run) requires collaboration between different countries. The servers are moved about frequently and in some countries (where the servers are placed temporarily) there is a lack of adequate legislation in this area. Often the service providers are themselves unaware of the criminal content. It appears that IP addresses are repeatedly sublet so that it is impossible to see in the end who the server is actually hosting.

This is not to say that closing servers is a lost cause. In 2007, for example, the Russian authorities succeeded in closing down a server which had provided its clients with virtual anonymity. This concerned the Russian Business Network (RBN). This provider of bulletproof hosting (servers that provide anonymity), based in St. Petersburg, was used a lot for cybercrime up to the end of 2007. Its closure provided food for discussion on the forum.

A member asked what had happened with RBN. It had apparently moved its services to other locations. One member, who used to be a client of RBN, agreed that they had simply disappeared. The most important consequence of the closure was that everyone had suddenly lost their provider. People who wanted bulletproof hosting had to pay more than what they were used to paying, whilst having to choose between various unknown providers. RBN is referred to as legendary and looked back upon as representing "the good old times".

Source: HTC interception

Still, setbacks only last for a limited period. In practice, one server is quickly replaced by another, after which the activities continue as normal.

Combating virtual convergence settings can also be achieved in other ways.

In the United States, infiltration of forums to ascertain the identity of offenders in order to arrest them have led to the dismantling of such boards. In 2008, for example, the forum DarkMarket came to such an end. It appeared that this English language forum, where credit card data was bought and sold, had for some time been infiltrated by the FBI. The infiltrator was even able to climb up to the important position of administrator, someone who acts as moderator in the forum.[6] In the end, this resulted in the arrest of 60 people in the UK, the USA, Germany and Turkey. Another example is the forum Shadowcrew, which was broken up in 2004. In that case, use was made of an administrator who had been arrested before and who then turned into an informant.

However, the use of infiltration is not sanctioned by law in every country. Furthermore, arresting authorities need the cooperation of several countries as forum members can live anywhere in the world.

There are also other solutions possible that could aim to reduce the value of the forum. A forum where mistrust predominates will be able to attract fewer market partners, resulting in a reduction in co-offending. Franklin et al. (2007) refers here to the principle of the lemons market, which is a market that suffers from asymmetrical information. The term lemon is borrowed from a car, with which everything went wrong (Akerhof 1970). Since everyone who buys a second-hand car is afraid of being fooled into buying a lemon, but often do not have the expertise to tell the difference between good cars and bad cars, this has a negative effect on the market price of second-hand cars. For that reason, the owner of a good car is forced to ask for less than what the car is actually worth. In other words, if users are not able to determine which providers are trustworthy or not, then the market will shrink.

Mutual distrust in the forum could hypothetically be fostered by intentionally saddling the forum with lemons. Such lemons can be introduced in two ways, by a sybil attack and by a slander attack (Franklin, Perrig, Paxson, & Savage, 2007).

In a sybil attack, the attacker creates different identities (sybils) in order to acquire a disproportional number of votes.[7] In the case of the forum, the aim of creating sybils is to undermine the status system. Franklin et al. (2007) distinguishes three stages in this process. At the first stage the investigating authorities must try to present as many sybils as possible to the forum. These sybils must then try to attain as high a status as possible during the second stage. This can be achieved, for example, by the sybils giving each other positive feedback, culminating in the verified status of trusted member. During the third stage the sybils offer their products and services to other members. If the sybils have a high status of trustworthiness, then it is likely that third parties will be interested in doing business with them. The trick is then to convince the third party to pay in advance, but to deliver nothing in return. This inevitably yields the status of ripper, but if the sybil has been careful in the way of attaining its verified seller status, then it is difficult to ascertain who is a real verified seller and who is not. This results in the market being undermined.

[6] http://www.theregister.co.uk/2008/10/14/darkmarket_sting/ and for an interview with the infiltrator see http://news.cnet.com/8301-1009_3-10234872-83.html

[7] According to Wikipedia, the term ‘sybil’ refers to a 1973 book by Schreiber called “Sybil”, in which a description is given of the psychoanalytical treatment of a woman with multiple personality disorder. The woman is referred to in the book under the pseudonym Sybil.

In a slander attack, the trustworthiness of others is attacked on spurious grounds (slander). The investigating authorities need to aim the attack in such cases at the market parties who hold a trustworthy status on the forum. Through their status, the trustworthy seller will have a comfortable position in the market. This means that he has sufficient demand for his supply and can therefore set his prices above the market rate. However, if his status falls, then his takers will no longer see the need to pay over the odds for his supply. They will then go in search of other parties who are prepared to accept a lower price for the same supply (although at the same time running the risk of crossing paths with other untrustworthy suppliers). In reaction to this the trustworthy seller will also have to lower his prices; he will no longer stand out as special and this will lead to him also losing clients.

A sybil or slander attack is limited, however, by the fact that it is not possible to pinpoint beforehand when sufficient mistrust has been built up in order to spoil the market effectively. Moreover, the following melancholic post from a forum member suggests that the collaboration in cashing schemes does not always run smoothly.

So you've decided to become a carder! Why? Lack of money? Or have you got time on your hands? Empty fridge, no regular work to be found anywhere and always short of money? So you happen to enter a site and start to read one article after another with growing interest, going from one forum to another, and you get the idea that this is a collection of super-intellectuals who simply by using their brains earn themselves hundreds, no, hundreds of thousands of dollars. And they're not even thieves, but genuine Robin Hoods, who steal from the shameless, fat, stupid bourgeoisie - Americans who are not worth their money.

If you're very lucky, then you will get your first USD 200 by the end of your second month. You're the lucky one! You're one of the 1000, perhaps as many as 5000, who've tried their hand at earning money by carding and for whom the attempt has succeeded (or who have at least earned back their initial outlay).

Plenty of others have suffered deceit at the hands of the card seller, money mules, money mule supervisors, the money provider or others. Carders have also been deceived by other carders! You might ask: "what do you mean… surely not deceiving your own mates?" To which I reply: "Naive boy". There's plenty of money to be earned from people like you! Not from cardholders, Americans, stupid money mules, but precisely people like you. (..)

Don't believe«father», nor«member of family», nor«Moderator», that's the law! Don't believe them! Don't believe anyone! Trust no-one! (….)

Source: HTC interception

Money mules

As shown by the cashing script, the money mules are an important link. They provide the casher with anonymity because they are the ones to break the money trail whilst at the same time running all the risks. This in turn means they form the weakest link. The money mules are, in fact, able to use their bank accounts once only, or at most just a few times, for channelling illegal funds. As soon as a victim checks their bank account details online or receives a periodical bank statement in the post, then they will discover the fraud and alert the bank. The bank can immediately trace to whom the money was transferred and block the relevant account. Recruiting new money mules is therefore an important condition to be able to continue cashing. In fact, it is probably the shortage of money mules that limits the losses incurred through high tech crime.

One method of prevention already in use is to alert potential victims via the radio and TV to the fact that cybercriminals are using spam to try to persuade people to make their bank accounts available. It is not known how much success this alert has; such campaigns are not accompanied by evaluation programs.

Another method of prevention is already being applied in the filtering out of spam messages. Spam filters can be specially programmed to be alerted by certain key words, such as 'financial manager' in relation to 'money transfer' or '5 %', and filter out such e-mails. This job description is often used to lend an official tone to this sort of recruitment e-mail.

It is also possible to approach the money mule market using the principle of a sybil attack. This method was accidently tested by HTC in the following way.

A member of the HTC received a recruitment e-mail in his (spam) inbox, which was asking for people to make their bank account available for use. In order to find out how the recruitment process works and thereby bring any vulnerability to light, he was given permission through the Public Prosecution Service to act as a potential money mule for this one time only. He therefore sent an e-mail back to the recruitment agency and in return was sent a contract together with instructions. Soon afterwards money was deposited into his account with the instructions to transfer this money in two parts to St. Petersburg. When he failed to send the money, he received three e-mails in short succession, demanding that he act quickly. He also received a text message ordering him to read the e-mails sent to him. When he failed to react to any of these messages, the recruitment agency stopped all contact with him.[8]

Apparently, the recruiter has no hold over his subjects. That is not strange. The carders are situated geographically at a great distance from the money mules, which means the carders are unable to resort to any physical powers. This appears to be a recurring problem for carders. A moderator from the 'problems' section started a discussion about unreliable money mules in the following way, where the members were invited to put together a blacklist of money mules who appeared to be con artists.

In connection with the apparent conning on the part of the money mules, I'm opening a special section for this subject. I'm attaching a format that should be completed for this purpose and I stress you should not to add unnecessary information: country, surname, address, telephone number, e-mail address, name of the bank, bank account number.

Source: HTC interception

The investigating authorities, in collaboration with the banks, could decide to create a lemons market of money mules. To achieve this, a large number of sybils would be created that would react to the advertisements for money mules. These sybils would, of course, not carry out the instructions concerning the transfer of the money. This would have the effect of flooding the market for money mules with unreliable suppliers. The carder becomes increasingly unsure of ending up with a

[8] The sum of money that was fraudulently transferred could be traced back to the original owner, so that the money could then be transferred back to him again.

credit balance. He will have incurred costs in setting up his cashing project. An added advantage in this situation is that if the identity of the rightful owner can be traced, then the money can be returned. However, if the rightful owner cannot be traced because the money trail had been broken at an earlier stage, then the banks could put the money aside, possibly putting it towards the costs of providing more effective advice.

Concluding remarks

Situational crime prevention can sometimes be very obvious. For example, consumers, shops and banks need to protect their payment orders in order not to fall victim to carders. This is so obvious, however, that it hardly needs a crime script to make such a suggestion. But in order to be able to come up with other measures, it is important to have a good idea about the crime script used by the offenders involved. What bottlenecks or chokepoints do they face? Only then it becomes possible to reconstruct the moments when offenders or victims are particularly vulnerable, or when supervision is lacking.

By using information from an internet forum solely dedicated to facilitating carding crime, one crucial bottleneck for cashers could be identified. That is the question of how to get hold of the money without coming into view of the investigating authorities. It certainly didn't appear to be difficult for cashers to make fraudulent money transfers, given the availability of malware and payment data. But transferring money from one account to another always leaves a digital trail. A casher cannot simply transfer money to his own bank account without this being seen. In order to break the trail, the casher therefore needs to use money mules. Judging from the discussions on the forum, these are difficult to find and are not always reliable. The government or banking sector could use this fact to their advantage. This varies from giving advice (government), using filters to highlight unusual patterns of payments by account holders (banks) or setting up false money mule accounts (government+banks). The last option has the additional benefit of making restitutions to the fraud victims involved.

Analysis of the carding forum also brings to light a second vulnerability. This does not so much concern one crime script or another, but is the recognition that the forum itself is of great importance. The cashing script shows that the carding/cashing process involves a high level of division of labour. Almost every stage requires a particular skill that is carried out by specialists in that area. These specialists do not know each other's true identities but find each other on carding forums. These virtual offender convergence settings, just as with physical offender convergence settings, can be described as specific meeting places where all sorts of information is exchanged, new criminal projects are set up and illegal goods and/or services are exchanged. Whoever gains admission to the forum thereby opens the doors to an enormous source of contacts.

An important theoretical implication of offender convergence settings is that they "allow criminal cooperation to persist even when the particular persons vary" (Felson 2006, p. 9). This means that certain places act as a gathering place for (potential) offenders. That function can then in turn lead to the creation of new contacts and

criminal projects. In this way a criminal network can be created that cannot be tackled by simply taking out a few people, who are designated as being important, because the overall view of the complete structure of the network is too hazy. There will always be people within the unidentified structure who can serve as a replacement.

The image that emerges from the forum seems to support this implication. The forum serves as starting point in the search for business partners for new criminal projects. Imagine that a criminal project is started, for example, the aim of which is to transfer money via European money mules. In such a project it is possible to identify the crucial links, people for whom the success of the criminal plans plays an important role. An investigation that is focused on these links will be able to disrupt the criminal project in question. It will then appear that the existence of a particular carding network has been hindered. But in truth this is not the case. That particular carding network was simply the result of the meeting of likeminded carders for a particular project. The forum itself, where they came into contact with each other, still sustains a much broader network in which dozens of crucial service providers are able to meet each other (virtually). Taking out one single service provider from one single carding project will therefore have little impact on future networks.

The literature shows that discouraging the use of physical offender convergence settings is important (Andresen and Felson 2010a, b). Tackling a virtual offender convergence setting is another way of looking at the problem of carding crime. First, it makes it more difficult for offenders to find suitable co-offenders. This can in turn reduce the number of crimes. Second, it impedes the accomplice regeneration process. Through the lack of meeting places, new recruits find it harder to gain entry to the existing offender population. Furthermore, the exchange of knowledge and expertise is impeded and the function of a criminal outlet for stolen credit card details or money mule services, for example, will be interfered with. When a carding forum can not be shut down (it is often difficult to determine jurisdiction if servers are constantly moved internationally), authorities should therefore set their targets at impeding the functionality of a forum.

References

Abadinsky H (1983) The criminal elite: professional and organized crime. Greenwood Press, Westport

Akerhof GA (1970) The market for “lemons”: quality uncertainty and the market mechanism. Q J Econ 84 (3):488–500

Andresen MA, Felson M (2010a) The impact of co-offending. Br J Criminol 50(1):66–81

Andresen MA, Felson M (2010b) Situational crime prevention and co-offending. Crime Patterns Analysis 3 (1):3–13

Ayling J (2009) Criminal organizations and resilience. Int J Law Crim Justice 37:182–196

Bichler G, Malm & Enriquez J (2011) Magnetic facilities: Identifying the convergence settings of juvenile delinquents. *Crime & Delinquency.* doi:10.1177/0011128710382349

Bullock K, Clarke RV, Tilley N (2010) Introduction. In: Bullock K, Clarke RV, Tilley N (eds) Situational prevention of organised crimes. Willan Publishing, Devon, pp 1–16

CBS (2010) Persbericht: internetters bezorgt over online dreigingen. [News report: internet users concerned about online threaths] Centraal Bureau voor de Statistiek, PB10-067, 26 oktober 2010.

Coles N (2001) It’s not *what* you know - It’s *who* you know that counts: Analysing serious crime groups as social networks. Br J Criminol 41:580–594

Felson M (2003) The process of co-offending. In: Smith MJ, Cornish DB (eds) Theory for practice in situational crime prevention, vol 16. Willan Publishing, Devon, pp 149–168

Felson M (2006) The ecosystem for organized crime, *HEUNI paper No. 26* (pp. 19). Helsinki: HEUNI.
Franklin J, Perrig A, Paxson V, & Savage S (2007, October 29-November 2) *An inquiry into the nature and causes of the wealth of internet miscreants.* Paper presented at the ACM Conference on Computer and Communication security (CCS), Alexandria, Virginia.
Heber A (2009) The networks of drug offenders. Trends Organize Crime 12:1–20
Holt JT, Lampke E (2009) Exploring stolen data markets online: products and market forces. Crim Justice Stud 23(1):33–50
KLPD/DNR (2010) High tech crime: Criminaliteitsbeeldanalyse 2009 (CBA). KLPD - Dienst Nationale Recherche, Driebergen
Morselli C, Giguere C (2006) Legitimate strengths in criminal networks. Crime Law Soc Change 45 (3):185–200
Peretti KK (2008) Data breaches: what the underground world of "carding" reveals. Santa Clara Comput High Technol Law J 25:345–414
Southerland MD, Potter GW (1993) Applying organization theory to organized crime. J Contemp Crim Justice 9(3):251–267
Trembley P (2006) Convergence settings for non-predatory "Boy Lovers". In: Wortley R, Smallbone S (eds) Situational prevention of child sexual abuse, vol 19. Criminal Justice Press, Monsey, NY, pp 145–168
von Lampe K (2009) Human capital and social capital in criminal networks: introduction to the special issue on the 7th Blankensee Colloquium. Trends Organize Crime 12(2):93–100
Zaitch D (2002) Trafficking cocaine: Colombian drug entrepreneurs in the Netherlands. Kluwer Law International, Den Haag
Zhang S, Chin K-L (2003) The declining significance of triad societies in transnational illegal activities: a structural deficiency perspective. Br J Criminol 43(3):469–488