**Humanising the Cybercriminal: Markets, Forums and the Carding Subculture**

**Craig Webber and Michael Yip**

**Abstract**

One of the more intriguing developments in organised crime is the use of social networking tools to facilitate relationships between like-minded individuals through the creation of discussion forums. Criminal tactics, tensions between rivals and self-reflection on a life involved in crime can now be studied, largely unfiltered and unaltered by the presence of a researcher. This chapter explores the social networking among cybercriminals and how carding forums act as enablers for global criminal networking. Through the study of real discussions on one of the earliest carding forums, ShadowCrew, this chapter also examines the mythical representations of carders and exposes, through their own words, the complexity not just of carding, but their motivations and life experiences. By doing so, we hope to expose a world that transcends rational choice and routine activities perspectives, so prevalent in the criminological study of cybercrime. In essence, the aim of this chapter is to highlight carding forums as critical facilitators of cybercriminal networking and in doing so, this chapter adds further support to the notion that cybercriminals are not the empoweredindividuals of lore, but instead, by exploring their activity through well-grounded criminological theories, we argue that this form of deviant behaviour, like any other, is messy, contradictory and often counter-intuitive. It is often far from rational. **Key Words**

Carding; Underground Forums; Criminological Theory

**Introduction**

*[A] carder can specialise in one or more areas of carding. But there’s nobody who does everything. Sooner or later that carder will need someone else’s services*

*Script [[1]](#footnote-1)*

Academic accounts of cybercrime base their theoretical foundation and explanatory analysis on various theoretical constructs such as subcultural theory (Holt 2007) and social learning theory (Skinner and Fream 1997). By far the majority of such studies fall within the rational choice/routine activities spectrum, both as explanations for cybercrime and for cybercrime prevention (Holt and Bossler 2008; Holt, Bossler and Siegfried-Spellar 2017; Leukfeldt and Yar 2016; Cohen and Felson 1979; Cornish and Clarke 1987). Few studies utilise an account that explains the thrill afforded by embracing subterranean values or the seductive appeal of ‘getting away with it’ (Matza 1964; Katz 1988; Ferrell 1999; 2013). Hence, many accounts utilise economic models to explain a phenomena that is against the law, carries risks of punishment and in many cases is hardly likely to net the perpetrator more than a well-paid job. In other words, carding is unlike most conventional jobs that rational choice models traditionally seek to explain. Consequently, whilst we do not deny the importance of certain elements of these economic models, we seek to use a more bounded approach to rationality (Kahneman and Tversky 1979), coupled with an appreciation of the seductive quality of the enterprise of carding derived from cultural criminology (Hayward and Young 2004, Hayward 2012, Ferrell 2013, Hayward 2016). Aside from learning the techniques of crime, it has long been recognised that it is also necessary to learn from others the “motives, drives, rationalizations, and attitudes favourable to the violation of law” (Sykes and Matza 1957: 664). Therefore, what follows is a discussion of data derived from conversations between carders on one of the earliest and most successful carding forums called ShadowCrew. These reveal the fluid nature of ‘techniques of neutralisation’, and which undermines any simple attempt at theorising motivations or over-reading the subcultural affiliations.

Our aim here is not to provide a quantified account where we seek to show the proportion of carders who hold certain views as opposed to others. One aim is to help in the disruption of the social scientific trend to replicate and build on similar work which leads to an imbalance towards one set of ideas over others. Our hope is to provide a ‘pause for thought’, to suggest some other avenues, some of which have already been taken to understand other areas of crime, but rarely in the area of cybercrime[[2]](#footnote-2). By examining online carding forums, this chapter approaches the subjects of this activity as both flawed and competent humans, some of whom are limited in their abilities, others who have lives that drift between the on- and offline world, thus challenging preconceptions about the mythical cybercriminal living alone and interacting with their computer as if they are a character living in *The Matrix* (Webber and Vass 2010). Unique to organised crime in a web-connected world is the use of social networking tools to facilitate relationships between like-minded individuals through the creation of online discussion forums (Benjamin, Li, Holt and Chen 2015; Holt 2017). This chapter explores one of the earliest and foundational of these social networking platforms and discusses how it acted as an enabler and template for global criminal networking. The key argument is that governments, law enforcement and security professionals have spent an increasing amount of money and time on chasing technological innovations to restrict, prevent and disrupt cybercrime. But, the evidence suggests that the web is only one aspect of the cybercrime environment, and that much of interest is missed when we ignore the human element of the activity. The goal here is to provide a “heuristic device, a rule of thumb” (Wall 2007, p. 34) for challenging the moral panic surrounding cybercriminals and highlight the influence of criminal and subcultural networking that occur on carding forums (Cohen 2002; Holt 2007; Levi 2009). Are cybercriminals as “empowered” as those portrayed in mainstream media? How did they discover the crime and start getting involved? Are they really nothing like “us”? Using discussions between the carders on the ShadowCrew forum, this chapter examines the perceptions, fears and triumphs of the carders themselves to get a glimpse of their way of life. This analysis adds to and supports the depiction of cybercriminals as complex, but also flawed human beings; in so doing we are not presenting an analysis that provides easy answers. Our aim is to nudge the discussion on the causes and consequences of cybercrime towards a more nuanced position where risk, thrill and excitement, as well as tedium and rational procedure, co-exist.

**Carding Forums and Subcultures**

The nature of cybercrime has been transformed by the rise of carding (Décary- Hétu and Leppänen 2016; Hutchings and Holt 2015; van Hardeveld, Webber and O’Hara 2017). The earliest successful sites such as CarderPlanet, formed in 2001, and DarkMarket founded in 2005, and the forum discussed here, ShadowCrew, founded in 2002, have been covered in detail elsewhere (see eg. Glenny 2011). But, it is accepted that they have become a template for many of the carding forums that have appeared since their demise (Lusthaus 2018). Carders are a specialised division of computer crime (Wall 2007) bringing money into the “cybercrime ecosystem”. They are mostly separate from, but interact with other branches of this network, such as hackers, spammers, phishers, malware authors, vulnerability finders, money mules, drops, and cashiers (Leukfeldt, Kleemans, and Stol 2016a; 2016b; 2016c; Lusthaus 2018a; 2018b). Most of these relationships are only ephemeral and akin to the arms’ length market relationships seen in commercial enterprises (Uzzi 1997, Brenner 2002). But, taken together, they give rise to a dark web of offenders, more often referred to as the underground economy (Leukfeldt, Lavorgna, and Kleemans 2017; Thomas and Martin 2006; Moore, Clayton and Anderson 2009). Failed and failing states, mainly from the former Soviet Union, produced eager recruits for these forums (Glenny 2011). Forum members can gain knowledge of how to ‘do’ carding, demonstrate their trustworthiness, and possibly move up the scale and into more respected positions. But, it is also apparent that there are smaller, localised groups that are culturally linked by shared histories. This is an important observation, because it adds to the argument that we need to see such groups not as some monolithic and homogenised mass, but as smaller, (sub)culturally specific hubs. This shares in common observations that have been made in criminal enterprises when networked technology was, at best, only peripheral (Hobbs 1998). Hobbs argued that there is a need to question the common analysis of organised crime that crosses borders as ‘transnational’. He suggests the need for an analysis that seeks to observe the local cultures of crime. The analysis of the human relationships on carding forums, and other similar networks, supports this contention, albeit with the proviso that networked communication systems allow for a far easier ability to connect with likeminded others, and learn the techniques needed to engage in the crime (Lusthaus and Varese 2017).

**Identifying common features on carding forums**

So, what can we learn from carding forums? Forums are a unique record of the conversations, business deals, tutorial sessions for self-improvement, and the residual human anxieties of those engaging in the buying and selling of stolen credit cards. It is where the offline and the online merge. Although we have studied many different discussion forums in the underground economy (Webber and Yip 2018; van Hardeveld, Webber and O’Hara 2017), data for this analysis was collected from the ShadowCrew forum, which existed between 2002 and 2004. This forum is used for the basis of this chapter as the authors were granted access to the complete forum data, including material that was only accessible to forum members when the site was live such as private messages. There are also ethical issues that need to be addressed in any replication of forum posts, but these are lessened with forums that have been taken down and obtained by law enforcement, and after ongoing investigations have been completed. There is a small, but growing literature on researching on the Internet and forums in particular, as well as the ethics of doing so (Wilkinson and Thelwell 2011; Hutchinson 2014; Sugiura, Wiles and Pope2017). The forum discussed in this chapter are all historical and no longer active, making this analysis akin to documentary research. In addition to talk of crime, these forums are venues for the discussion of topics that have a more mundane, off-line quality, such as where to buy illegal drugs, or what protein shake is best for muscle gain. These forums provide insight into the life that is lived outside of carders’ computers and outside the purpose of the forum’s original creation (Webber and Yip 2012). There are exchanges that raise questions about the morality of the theft of credit cards; rivalries explored and status negotiated; and fame sought despite the dangers of raising one’s head above the firewall. Of course, it is unwise to only use such forums for data and to treat them uncritically. However, they do have the benefit of being data unsolicited by a researcher.

Forums are generally accessible to all, but carding forums often have the additional element of an invite-only system restricting certain areas of the site to those most trusted. This allows the carders to establish a boundary between them and the rest of the Internet. Inside these “virtual walls” is a society of carders bounded by the common goal of a profitable return from carding and governed by the forum administrators. In essence, and in an echo of traditional British subcultural theory, a carding forum is “an organized set of social meanings which presumably bear some relation to a larger more inclusive set called ‘the culture’” (Clarke 1974, p. 429). However, we need to be careful not to think of the whole carding subculture as overly homogenous in their values. Aside from a goal of using stolen credit card data to commit fraud, the reasons for doing so can be varied, and so make descriptions of the overly rational and calculating cybercriminal less easy to sustain as a catch-all explanation. The goal of this chapter is to discuss the social meanings within the ShadowCrew carding subculture and to demonstrate how the values are reflective of cultural norms in both criminal and legitimate settings. This is achieved by breaking it down into a set of *normative orders*, defined by Steve Herbert (1998, p. 347) as a “set of generalized rules and common practices oriented around a common value”. An order “provide[s] guidelines and justifications” (1998, p. 347) for behaviour, although they are not assumed to be prescriptive, thus highlighting the impact and influence of subcultural membership on the carders. We have arrived at the normative orders through our analysis of various forums and from reviewing the literature in both organised crime and cybercrime. Holt (2007) argued that only three subcultural normative orders have been consistently identified across studies of hacker subcultures:

* *Technology*: An almost intimate relationship with technology, sometimes referred to as an addiction, coupled with the innovative adaptation of technology to novel applications.
* *Secrecy:*  Since hacking is illegal, secrecy is a key requirement, but equally reputation is built on successful exploits notified to hacker communities in online forums.
* *Mastery*: The learning of new skills and control over technology and environment.

However, in this analysis, we treat these as underlying narratives in the sense that they are foundational aspects of many forms of cybercrime. We have focussed on five factors that we will argue are integral to carding and highlight the difference in this activity to that of hacking for fun, excitement or challenge. In addition to Holt’s three normative orders, our focus is on an additional five normative orders: *networking*, *competence*, *drive*, *morality* and *duality*.

* *Networking*: an essential part of carding, it is important to proactively establish connections with other carders.
* *Competence*: given the risks associated with carding, it is important for carders to master the techniques of crime. As carding relies heavily on trading, it is also important for carders to be resourceful and have something to offer for trade. Even if one does not possess stolen credit cards for trade, a competent carder could still trade for skills, knowledge and experience (see Yip, Shadbolt and Webber 2013 for a fuller discussion of this).
* *Drive*: most carders appear to be driven by materialistic goals but some also find carding a thrilling experience. Key here is the argument that whilst rational economic calculations might be made by some carders, many would still card if they were offered a well-paid job using those same skills for good, not ill.
* *Morality*: whilst some carders are willing to use whatever means to earn quick money (e.g. scamming college kids), some have shown moral boundaries by only committing carding crimes as they believe the fraud victims are not the individuals but the big banks which they blame for seducing the society into financial debts.
* *Duality*: carding is different from other forms of cybercrime such as hacking as the crime necessitates the carders to commit crime in real-life. This means that carders have a need to be able to maintain composure when they encounter difficulties during criminal acts (e.g. withdrawing from stolen bank accounts).

This chapter is not about how networks grow, but about the ways people behave whilst on carding forums and the fine detail of how they respond to each of these normative orders. Each order works together, but is also mutually exclusive. So someone can be well connected on a network, but be relatively poor at carding because they do not have the drive or competence. Equally someone may justify their carding through what they perceive as a high moral code, so they only commit fraud against people they think deserve it, whilst others are only motivated by profit regardless of the target’s ability to afford the loss. We also employ a variety of criminological ideas to help us understand the phenomena in question, and do so with an attitude of theoretical promiscuity. Older theories and more contemporary thinking combine to become a heuristic device to help us think about a phenomenon that shares many characteristics with established forms of criminality, but which in many other ways is also unlike traditional forms of theft or fraud. Therefore, the social network that emerged on ShadowCrew is treated as a cybercriminal subculture, one which provides opportunities for the social learning of the rules of carding through what Edwin Sutherland termed differential association (Sutherland 1939). But, it also provides a support network that enables, encourages and councils those who use it.

**‘For those who wish to play in the shadows’: The early development of the techniques of carding.**

The carders of ShadowCrew shared an ethos of play, innovation and ‘gaming the system’ with the wider community of hackers, and is epitomised by ShadowCrew’s banner: *For those who wish to play in the shadows!*. To succeed in carding, it is important to master the “tricks of the trade”. But, key here is the playfulness expressed, the same kind of seduction in the evolving competence that the forums were able to promote through their ability to provide tuition and guidance without parallel in traditional organised crime. Rarely were the techniques of traditional organised crime written down in easily accessible tutorials. Now, the risks of harm from networking opportunities were reduced, in contrast to what might be the case in a late-night discussion of a criminal opportunity in the car park of a pub or bar. But, to avoid detection and prosecution, standards still need to be maintained. This section examines two normative orders that are central to carding: *networking* and *competence*.

***Networking***

One of the most common characteristics in the depiction of cybercriminals is their individualistic nature. Cybercriminals are often represented as talented but lonely individuals who are capable of wreaking havoc. As Wall (2007, p. 40) describes them, they are “lone offenders who exploit networked technology to carry out incredibly complex and far-reaching tasks that can be repeated countless times globally”. Based on observations from ShadowCrew, however, such a depiction prevents us from recognising online criminal networking as one of the most important transformative impacts upon criminality. To highlight the process of financially motivated cybercrime, this section draws upon a carding tutorial that was posted on ShadowCrew in 2002. Forum discussions are based on an instant messaging system that tends to involve slang and typos. Where possible, the original message is kept verbatim and only the layout is altered. Consequently, there will be errors of syntax, grammar and spelling.

The author began the tutorial with a side note that suggests that the tutorial was originally written for another forum and encourages the readers to correct mistakes. This highlights the sense of freedom carding forum members enjoyed and the sense of community felt among them:

SIDE NOTE: I originally wrote this C+/B- FAQ for another smaller board, but I dont mind sharing it. I would appreciate it if someone informed me if any statement is made in error on this faq: I dont want to be that kid walking around with a big booger in his nose and instead of telling him, ppl just point and laugh or nod and smile Shocked creepy.

----

This FAQ is intended for educational PURPOSES ONLY. If youre a federalle[[3]](#footnote-3) and youre reading this, you better be educating yourself or I've got a big lawsuit against the United States Govnt.... I'll settle for a "get out of jail free" card though :\

The author then proceeds to define what carding is – “the art of credit card manipulation” – and that common motivations for entering the crime include poverty and thrill. This suggests a sense of thrill-seeking, perhaps even a compulsion or addicition, for mastering the crime, rather than just for financial gain:

- Well, defined loosely, carding is the art of credit card manipulation to access goods or services by way of fraud. But don’t let the "politically correct" definition of carding fool you, because carding is more than that. Much more.

Although different people card for different reasons, the motive is usually tied to money. Yea, handling a $9,000 plasma television in your hands and knowing that you didnt pay one red cent for it is definately a rush.

But other factors contribute to your personal reason for carding. Many carders in the scene come from poor countries, such as Argentina, Pakistan, and Lebanon where $50 could mean a weeks pay, on a good day. Real carders (the ones that have been in the scene the longest) seem to card for something more, however. The thrill of cc[[4]](#footnote-4) manipulation? The rush that the federalles could bust down your door at any minute? The defiance of knowing that everyday that you are walking among the public is another day that you’ve gotten away with a federal crime?

Whatever your personal reason for carding is, this tutorial should answer a few noobie[[5]](#footnote-5) questions and take the guessing out of the entire carding game. The resources and techniques mentioned in this tutorial are NOT, I repeat, NOT the only methods of carding. Experience in carding is key. You have to practice your own methods and try out new techniques in carding to really get a system that works for you. This tutorial is meant to get you on your way.

The author then proceeds to explain how to obtain credit cards either through (1) “ripping” – dishonestly trading and defrauding other carders, (2) database hacking, (3) or trading, which is suggested as the easiest way to obtain stolen credit cards:

Credit Cards: Yes, CCZ. I cant count the number of times someone has messaged me with:

"do you have any ccz"

"where can I hack CCZ"

"where can I get a list of valid CCZ?"

You need money to make money. Plain and simple. Which means that the only way youre gonna be able to get ccs if you have ABSOLUTELY NO MONEY is if you successfully rip a noobie with 100 cards (but what noobie has 100 cards?), if you have any background in database hacking, if you trade for your shit, or if you know someone thats willing to give you ccz all day.

I know thats a discouraging statement to all of you, but we have to keep shit realistic. The easiest way to get ccz is to purchase them.

Readers are also reminded of the need to be resourceful and always have something to trade:

If youre REALLY strapped for cash, you have to go through the alternative: trade for your resources. you have to be resourceful in carding, meaning you have to use what you got. Got a psybnc[[6]](#footnote-6) admin account? Offer psybnc user for a cc or two. Got shells[[7]](#footnote-7)? roots[[8]](#footnote-8)? Can you make verification phone calls? just ask yourself "what do I have that might be valuable to someone else?" and work with that. It doesn’t have to be big, it just has to get you a few cc's in your palms.

Once youve run your first successful cc scam, DONT SPEND ALL YOUR EARNINGS. Save $200 and re-invest back into the carding community. head to SC[[9]](#footnote-9) and get better cards. If you have level 2 cards, I suggest carding C2it/Paypal and using that $$ to buy ccs. (successful C2it/PP scamming techniques will not be discussed in this tut, sorry)

It is important to recognise that trading implicitly requires criminal networking with others, exposing the cybercriminal to the potential danger of encountering rippers, the term used to describe a cybercriminal who rips off or commits fraud against another carder, or undercover law enforcement agents. This shows that unless you have all the skills required for carding, from stealing credit cards to money laundering, trading is inevitable. Who should one trade with? How should one establish trust[[10]](#footnote-10)? The author then introduces ShadowCrew as the venue for trading. ShadowCrew is a place where mistrust is managed and where people with similar criminal dispositions collude. In essence, a forum like ShadowCrew satisfies the two predominant requirements for exploitable criminal ties to emerge (von Lampe 2003): *meeting individuals with corresponding criminal disposition* and *a common basis of trust,* as shown below.

ShadowCrew reviews all sorts of merchants and sellers of any type of service imaginable (everything from selling full-info cvvs with changeable billing addies[[11]](#footnote-11) to purchasing anonymous bank accounts. If you dont know ShadowCrews forum link, ask someone.)

…

ShadowCrew (where the big boys play) is an unreplacable tool for todays carder. ShadowCrew is not for newbies. They discuss everything from cc fraud to anonymous bank accounts, identity theft, scams, fraudulent passports, etc.. (The first time I logged on I couldnt believe the amount of fraudulent activity taking place there. I wouldnt be surprised to see Bin-Laden hanging around in there ). Their forums are extremely useful and they rate and review their sellers so you know the service youre getting is legit.

Be careful of people out there... between federalles and rippers, the carding scene is a shady place. But if you know how to handle yourself and play it smart, you'll get some good results from the dedication you put into carding.

In order to avoid rippers, it is important to be able to validate the credit cards in possession and check the balance of money in the account. The author of the tutorial recommends a few methods, but it appears these are hard to come by:

Knowing whether your cc is valid or not is really important for saving some time and energy. If you live within the USA, theres a phone merchant posted within this forum under (cvv2's and ccs).

The ideal way for checking ccz is through an online merchant. These merchants can verify cc amounts without charging your ccs. Good luck finding one. People on IRC[[12]](#footnote-12) want a ridiculous trade for these merchants (cvv lists, cash). So if you run across a legit merc, dont give it out! even to your best buds! online mercs are gold in the world of carding.

Other methods for verifying cc amounts include registering your cc on an online bank. (You will need at least a level 2[[13]](#footnote-13) card, level 3 for ATM cards). alot of online banks can give you limit, billing addy, etc. etc. but they require at least a level 2 cc (more info on ccz below)

Once valid stolen credit cards are in possession, the next step is to defraud the accounts. This requires personal information about the cardholder. The amount of personal information associated with the stolen credit cards is categorised under three levels:

I want to make something clear right now. The secret to carding is not the number of cards you own, its what you can do with the cards. What do I mean by that? Simple.

Hypotherical situation: My name is Johnny and I have 3 ccs with SSN[[14]](#footnote-14), DOB, CVV NUMBER, MMN, NAME, STREET ADDRESS, CITY, ZIP, AND BILLING TELEPHONE NUMBER. I have a friend named Billy. Billy has 300 CCCZ with CVV, MMN, NAME, STREET ADDRESS, CITY, ZIP, AND BILLING TEL. NUMBER. Whos more likely to successfully card something?

Simply put, I (Johnny) am. Why? Because I have more information that can prove that I am the person who owns this CC than Billy does with his 300 CCVZ. Does that mean Billy's not gonna card anything? No, that just means Billy's gonna have a hard time carding anything without verification.

So to sum up this lesson, you have to get information on your mark (the person that youre impersonating.) #1 rule in carding is: the more information you have on a person, the better chances you have for a successful transaction. Here is the information you're looking for (note: the levels of a card is not a technical carding term, I just used L1 L2 L3 to simplify shit throughout the tutorial.) :

NAME:

ADDRESS:

CITY:

STATE:

ZIP CODE:

TEL. BILLING NUMBER:

CARD NUMBER:

CARD EXP DATE:

CVV CODE:

(The above is LEVEL 1: REGULAR CVV. If you have this much info, youve got yourself a regular cc. Nowadays you need this much info for carding ANYTHING worth mentioning. If you have any less than this information, youre shit outta luck. :\)

Social Security Number (SSN):

Date Of Birth (DOB):

Mothers Maiden Name (MMN):

(LEVEL 2: (PARTIAL FULL-INFO) If you have this much info as well, your ccz are on another level. With this info, you should be able to card PayPal, C2IT, and other sites without too much of a hassle.)

BANK ACCOUNT NUMBER:

ROUTING NUMBER:

BANK NAME:

BANK NUMBER:

DRIVERS LICENSE NUMBER:

PIN NUMBER (For CC or ATM card)

(LEVEL 3: (true full-info) If you have this info as well as Level 1 and 2, youre cc is ready to card anything your heart desires)

However, the process of fraud cannot begin without adequate protection to preserve anonymity and the ability to eliminate evidence when needed:

Safety is key. No one wants to give the federalles the satisfaction of busting us and shutting down production, so we gotta stay as anonymous as possible.

First let me start off by saying theres no 100% safe way to card. Dont let people fool you into thinking that. You can be behind all the proxies[[15]](#footnote-15), wingates[[16]](#footnote-16), socks[[17]](#footnote-17), and whatever else in the world, but you leave "digital fingerprints" wherever you go. I use a private hidden proxies, and dont really fuck with any other proxies, so I cant comment too much on this topic (maybe someone will paste a separate proxy faq?) As far as I'm told proxies differ from level 1 to level 3, 1 being the most anonymous, 3 being the least.

If you're really serious about carding, this is program, *PoloMint[[18]](#footnote-18),* you NEED to have installed on your HD[[19]](#footnote-19) at ALL TIMES! Federal agents have several programs that allow them to extract information from your PC, such as the pages you have visited, the files you have deleted, and the emails you have written. Everytime your PC restarts, *PoloMint* kicks in, providing you with the safety of erasing any tell-tale logs and history files. You always want to be prepared for the worse.

Once ready to defraud stolen credit cards, the next step is to find physical addresses (drops) that can be used as delivery addresses for proceeds of fraud:

The right drop is essential to your scamming needs. Finding legitimate drops inside and outside of the US is hard. Many people keep your shit and dont send, or some people dont pick up the package at all! (theres nothing worse than watching your hard-earned laptop going back to the store because it was refused by the recipient)

If you live inside (or even outside) the USA, youre better off scoping a drop out on your own. A drop is basically an empty home that looks to be inhabited. This is the shipping address you use for your carding needs. Your items should only picked up at night. As always, be sure to have a cover-story in case someone asks why youre snooping around an empty home. "I'm picking up a package for the person that used to live here" is a legit excuse. Or even "my father is the real-estate agent." is good.

Although this tutorial did not cover every aspect of carding, such as card cloning and money laundering, it has shown enough to demonstrate that making a profit in carding is a process that requires many different kinds of resources including stolen credit cards and the associated personal information, drops and secured proxies, as well as knowing which websites to defraud. Evidently, carding is a highly complex crime that requires those engaged in the crime to obtain access to many different types of criminal resources (including intangibles such as techniques and experience). This highlights that there is a limit to what an individual carder can achieve, and so to earn a profit in carding, more than one person is likely to be involved.

Unlike in conventional crimes where access to criminal resources is often restricted by physical and geographical constraints, carding forums allow cybercriminals to meet others anywhere, anytime. Coupled with the instantaneity offered by the Internet (Sandywell 2010), carding forums greatly expand the resource pool that is immediately available to cybercriminals. This is a critical characteristic of financially motivated cybercrime.

***Competence***

However, as highlighted in the tutorial, carding is a trading business and carders have to be resourceful so they have something to offer for trade. Furthermore, carding is a risky business. One wrong decision and it could result in being caught by law enforcement. Therefore, mastering the techniques of crime is essential to becoming a successful carder. This is evident from the responses to the tutorial described above highlighting just how important learning is in carding and the level of commitment some carders have shown:

Amazing tutorial, I've been covered to most of the things you mentioned by reading hundreds of tutorials, but all of that knowledge in one tutorial is a great save.

*Hax0r123*

---

Yea, the only thing I would add is make sure you do your online shopping at a public library, Internet cafe or college library.

And be ready for a phone call for high dollar stuff.

Also, knowing the cc balance is key.

Great post though.

*MrChill*

---

Lovely post, helpful to those starting out. Good starting point.

I will add a small point that I am noticing alot lately.

..

I find quite a bit that you will need to talk to the credit or fraud department of the particular shop you are ripping, and convince them of your intentions and identity. For many stores now, they will check the phone number that you have provided (cell or whatever) against a database, including doing an online search for your phone and address. They tell the carder, that phone number is a cell phone. Sorry can't help you.. Or your address is coming up as a mail service or box location, even though you checked the drop to see if it is in database, and it wasn't.

So a lesson or two about this that may or may not be helpful. Instead of using an anonymous cell phone, get a prepaid Master Card or Visa and sign up for a Voice Mail service and leave a message like it is your home number. Advantage;;;;; this number will not show up as belonging to a cell number, it just won't show up. You tell them you have only had the line for less than two weeks, so you might not be listed...A little more of a pain is going to pay phones constantly to call in to the vendor or CC company.

Hope this helps someone..

*the\_unknown*

The responses to the tutorial above show that in order to take advantage of new and developing criminal opportunities, carders have to keep up with technological innovation. This is further supported by responses to a thread which calls for a new sub-forum for those who are new to carding:

just do like most of us here have. read, read, read. start reading the oldest posts here in this forum, and go on. you really learn a lot by just paying attention, and reading all the posts. i'm by no means an expert, but this is how i have learned most of what i know about id's, cards, and creating identities. there are also links to tutorials and long text files in some threads, in addition to the tutorial section. THEN, start asking questions, cause most of it's already out there. good luck!

-Roger-

There is so much knowledge and talent here ..but i think a newbie forum is kinda like free 24 hour room service w/a 5 star 5 diamond menu...come on man.

~~NiHao~~

When this tutorial was written in 2002, Amazon and similar websites were still in their early stages of development. High priced items now need to be signed for, and increasing levels of security are common place, rendering an empty drop problematic. Now, a high-priced item is unlikely to be left at a house. Instead, it would likely be returned to the sender, or left at a local shop or post-office and require a signature and photo identity with an address matching that to which it was sent. ‘Cashing-out’ credit cards to turn them into usable or sellable goods, or cash, has developed significantly since this period. The buying of cryptocurrency, such as bitcoin, effectively using credit cards in order to turn a stolen identity into anonymous money, has become a more commonplace endeavour than buying goods such as computers and televisions to sell-on.

From the contents of the tutorial and the responses relating to learning the “tricks of the trade”, the learning includes not just the technical skills such as checking the balance of credit cards but also the *argot* of the carding subculture, “a specialized and secret language within a subculture that serves multiple functions within the group, such as communicating the structure, norms, and values of a given subculture to its members” (Holt 2010, p. 467). Abbreviated terms such as CCZ, Full-info and CVVs are some of the terms commonly used and which define this subculture. Carding forums like ShadowCrew serve as venues for carders to meet, trade, and most importantly, engage in dialogue that allow them to share current techniques and experiences.

In order to understand carding fraud and to humanise those behind it, questions are asked of the data such as: Why did they choose to become a carder? Do they have moral boundaries? Are they criminals in ‘real-life’?. In doing this, we will explore the last three normative orders of *drive, morality* and *duality*, respectively. It will be argued that although there are economic rationalities expressed by the carders to explain their engagement in this fraud, this is bounded by subterranean values of thrill-seeking and resistance (van Hardeveld, Webber and O’Hara 2017). From this thread, it can also be seen that there are a number of key recurring themes in the motivation of carders:

• The desire for higher social status and easy money.

• The lack of legitimate ways to achieve higher social status, due to previous wrongdoing.

• Peer recognition.

• Habituation to the lifestyle of the underground economy, often referred to as an addiction. We need to be careful with medicalised terms like addiction. But, we report the discussions of the carders who use this term frequently.

• Duality; disconnection from offline society.

Each of these five points will be discussed in relation to the three remaining normative orders; drive, morality and duality, with ideas derived from cultural criminology used to help form a better understanding of the carders and the influence of subcultural membership.

***Drive***

From a conversation under the topic “Do you have any regrets” on ShadowCrew, some answers to the question of what drives and motivates carders can be found, but we also see that these normative orders can overlap in significant ways. Here the drive to commit this form of fraud is often couched in terms of trying to overcome regret at the choice to pursue this activity:

Some parts of it I love. I'm a total loner outsider, some by choice and some by the fact I've never been the type of guy that gets the girls or anything. Doing what I'm doing kind of makes me feel like I'm doing something...something a little risky...then when I do something, I still sometimes feel guilty about the people I'm doing it too. I hate that part of it. I'm never going to have a normal life even if I try, so this life, as ShadowCrew says,‘For those who wish to play in the shadows[[20]](#footnote-20)’ I love the shadows. I love doing things in the shadows. That's where I'm comfortable’.

*TheDevil*

*---*

I agree, it gets addictive. There is always that feeling of trying to be the best between your shady friends but appear as the second (because the number one always get caught)… Anyway we are free to choose our lifestyle for a while, and most of us are here because we like what we do or what we get from it. That's my opinion

*\_cracker\_*

---

In a lot of ways I regret where I am at today. When I was younger I didn't realize the consequences of the shit I was doing - easy money was great. But once you get a record and your chances of a good legit life slip further away the less choice you have in the matter. Now that I am older I wish I had done things differently, but this is the life I chose & as long as I have to live it - I am going to try to take it as far as I can. I am hooked on the rush - there have been times when I could have resumed normal living with a 9 - 5 job, but I could never bring myself to do it. I need the excitement & the fast cash. The stress is just something I have to live with - that and the isolation from everyone else. With the amount of time that I put into my ’job’ there is hardly any time to enjoy life - but it's addicting.

*Rupuze79*

---

I agree with Rupuze79: once you get older and get a record, legitimate jobs become that much harder to obtain, thereby making this life that much more attractive. I've concluded that the only way I can make a decent living legit is to own my own business. Since the banks won't give me a loan I have to 'give' myself one. My only regret in this life is doing time. As for it being addictive; everyone needs an exit strategy. Even the Kennedys eventually went legit. Also don't forget where the real money is and where the real crooks are, is in legit businesses.

*Dr. P*

---

I try to have the fewest regrets possible. There is nothing you can do to change the past. What's happened has happened. My biggest regret? Not putting in the effort in High School and college. Looking back I wish I had done well enough in High School to go to an ivy league school. From there I could have made contacts and moved into the legit business world much quicker. Once you get a taste of the easy money it's hard to let it go.

*JediMaestro*

Cybercrime is often suggested to be an easy way to quick money with relatively low risk of getting caught (Wall 2007). In his thesis on social structure and anomie, Merton argued that certain social structures exert a definite pressure that triggers impulses to break social controls (1938). Two elements are particularly relevant to carders: culturally defined goals and the acceptable processes for achieving those goals. Since cultural goals are often couched in economic terms and cybercrime is often portrayed as a lucrative crime, it is reasonable to hypothesise that cybercrime would appear as an attractive route for those seeking to achieve higher social status through the acquisition of money or high value goods. As Cloward and Ohlin (1960) argued, however, there is differential access to legitimate routes for achieving culturally accepted goals and therefore, some choose to pursue criminal routes instead of legitimate ones. This attitude is shown in the response of a carder, ForeverYoung:

one thing you mention is that carding isn't always that easy, its not like you can roll outta bed and card shit. It does take some prep work, the more the better if you want to stay free.

I would add keeping carded merchandise is bad news, flip it for cash and make sure the belongings in your home are legally yours. I know that if you're young and can't really afford the finer things in life (ps2s, dvds, etc) carding is just about your only option. Keep any carded items hidden from parents, or find a way to convince them you bought it - "look ma, I bought this x-box at a garage sale!" Instead of carding an entire PC, just stuff your old beat case with the latest boards, no one will ever know.

For the newb its better to take it slow at first, get a feel for it before jumping in with both feet and getting burned.

*ForeverYoung*

In reality then, some carders are the opposite of the deviants commonly depicted in cyberpunk cultures that have “little control over their own eventual fates and are constantly struggling to assert their individuality” (Taylor 1998: 406). Instead, some carders appear to be self-evaluating, reflexive individuals who know what they need to do in order to achieve what they regard as socially accepted goals. Rather than being “constantly struggling to assert their individuality in the face of the identity-threatening technological systems” (Taylor 1998: 406), it appears that some carders use carding as a means to achieve their personal goals. To these carders, carding is just an illegitimate route to the “American Dream”, or any other national dream of success, and they have made a rational decision to go down such a route. While media-manipulated moral panics require that we see people like the carders as “others”, the desire of carders to achieve a socially accepted goal (rather than a deviant one) would likely make them more understandable to many. Consequently, in these responses, we see the synthesis of thrill seeking, consumerism and neo-liberal wealth accumulation, echoing conventional routes to success. It is Merton’s innovative mode of adaptation joined by Matza and Sykes’s subterranean values (1961). Indeed, some would argue that this is the very hypocritical nature of exploitative capitalism that we define as deviant those elements of activity that we see as a threat, whilst allowing others to be defined as legitimate despite their social costs (Hall and Winlow 2007; Winlow and Hall 2016).

This is not to dismiss the possibility of the loss of individuality entirely. As shown below and in other threads presented in this chapter, there appears to be a common attitude towards carding as a form of addiction, obsession or dependency (see earlier responses by \_cracker\_ and Rupuze79), and it is possible that some carders are subsumed by the thrill resulting in a loss of self-awareness and, subsequently, self-control:

Naah, carding definitely isnt easy, but then again I wouldn't have it any other way. Why is that? simple. That's my adrenaline rush in the madness of things

anybody can copy and paste. the real thrill of carding is successfully manipulating the system. Or at least thats my personal interpretation of the enigma... I'm sure most people card for the money, but I card for the luv....

*Invincible*

The repeated mention of the thrilling sensation of carding is evident from the conversations above and this thrill of carding appears to be one of the defining experiences and emotions of all forms of crime (Ferrell 1999, p. 404). Some carders, like *Rupuza79*, appears to have gone as far as rejecting legitimate routes and have been fully seduced into committing carding by the moments of “sneaky thrills” (Katz 1988). This thrill-seeking behaviour has also been seen among computer hacker subcultures as Jordan and Taylor (1998) found:

…hackers often confess to an addiction to computers and/or to computer networks, a feeling that they are compelled to hack. Second, curiosity as to what can be found on the world-wide network is also a frequent topic of discussion. Third, hackers often claim their offline life is boring compared to the thrill of the illicit searches in online life.

(Jordan and Taylor 1998: 768)

In essence, what is evident from the discussion threads examined is that the carding subculture consists of people who have come to carding for a variety of reasons. Some have closed off their legitimate routes to success due to previous convictions, others appear to have limited access to legitimate routes and resort to carding as a way to finance their access to a legitimate route. Some appear to be hooked on the thrill of the crime and express a compulsion to pursue the illegitimate route. This observation concurs with Albert Cohen’s remark:

Those who join hands in deviant enterprises need not be people with like problems, nor need their deviance be of the same sort. Within the framework of anomie theory, we may think of these people as individuals with quite variant problems or strains which lend themselves to a common solution, but a common solution in which each participates in different ways.

(Cohen 1965, p. 8)

In carding subcultures, members with different backgrounds have found carding as a common solution to their personal problems and in the process, many encounter the pleasure of an “adrenalin rush”. Thrill is a significant characteristic of membership in a carding subculture, just like that in a computer hacking subculture (Jordan and Taylor 1998; 2004; Holt 2010). It is not possible in this study to determine the significance of thrill in pushing or pulling someone into credit card fraud. Whilst thrill may not be enough to seduce someone into committing credit card fraud in the first place, it may well play a vital role in seducing carders into reoffending (McCarthy 1995). In other words, the ability of an individual to make a rational choice (Cornish and Clarke 1986) about committing credit card fraud may differ before and after crime has been committed. Once the individual has had the first taste of carding, the thrilling sensation may overwhelm their ability to self-control (Gottfredson and Hirschi 1990), thus clouding their ability to reason rationally and assess accurately the risk of being caught by law enforcers and the associated consequences (van Hardeveld, Webber and O’Hara 2017). The point is, although rational choice and routine activity perspectives are often used to understand how one might prevent cybercrime offending and victimisation, they are less well-placed to explain the complexities that drive further offending.

***Morality***

First introduced by Sutherland (1939) and advanced by Akers (1977; Akers, Krohn, Lanza-Kaduce, and Radosevich, 1979), the theory of differential association argues that criminal behaviour is learned by being in association with other criminals. Indeed, how-to tutorials such as the one described in the previous section are commonly available on carding forums (van Hardeveld, Webber and O’Hara2017), but this is not the only thing that is learned. As Sykes and Matza (1957) argued, juveniles become delinquents only after they have learned the techniques of neutralisation to justify their deviant actions. This process of learning to neutralise actions is evident from replies to a topic about scamming college students:

I agree, scamming college children is plain and simply wrong... thats their real hard earned money and there's no way for them to get it back... Credit Card fraud, the victim gets all his money back... it's a victimless crime, but this is just plain wrong... I'm not flaming you, I'm just saying, I'd feel better if you see my point of view and please not do that again. Sorry to put you on the spot like that, but it's just my opinion.

*Fe@r*

*---*

Yeah just cuz the world is immoral doesn’t mean we have to feed that fire I personally like to get credit card companies who get the young people dooped (duped) into school loans and credit cards and then not having a way to pay it back. when its time to work and make a living they come for the money and make your life a living hell. so screw them Robin Hood style.

*Camp*

From the above dialogue, it can be seen that the carder named Fe@r attempts to “deny the injury” (Sykes and Matza 1957: 667) by claiming that credit card fraud is a victimless crime as the victims are likely to get their money back. Additionally, Camp attempts to “deny the victim” by believing that credit card companies deserve his fraudulent action as they cause young people to be in debt. This dialogue also supports Sykes and Matza’s argument that delinquents are at least partially committed to the more widely accepted conventional norms and values as it appears that carders are in fact driven by goals similar to those of mainstream culture.

Members of the forums are able to read each other’s justifications and this has the effect of reinforcing their own beliefs. Some carders know that their actions are morally wrong; however, the lure of quick cash and the possibility for victims to get compensation is enough for them to justify their actions. It appears that their actions are justifiable as long as the big corporations take the losses and not the individual owners of the credit cards:

I'm not here to lecture, but I'm interested in the morality of ripping people off in auctions. I can understand why you may want to make £ from large retailers and CC companies, but do some of you feel guilty if you take say a postal order or cheque from a buyer on ebay and don't send an item? I know they have a fraud policy but it only covers low amounts. Personally I wouldn't do anything like this, unless it was perhaps to get back at someone or out of desperation. Another reason is that the more fraud that is committed the tighter the laws and security will become, as long as its worth the company's time and money, not to mention the already long sentences for stealing something which never physically existed. It also makes it harder for people to use it for positive reasons (ie anarchy against a corrupt regime or desperation), which I suppose depends on the mentality and angle of the person. Just a few considerations. Any comments?

The\_place

---

I agree it isnt a particularly nice thing to do to people, but you can get several k[[21]](#footnote-21) from a couple of hours work, so its easy to see why people are doing it.

If you feel bad about doing it just use paypal then people can file chargebacks with their cc company and visa will eat the loss.

cheers

fw

---

At the end of the day its a shitty way to earn a living but like fw said its easy money and if you only accept payments through billpoint/paypal then its the big companies who take the loss. Morally its totally wrong, better to just accept that than trying to justify it with 'positive reasons' (ie anarchy against a corrupt regime or desperation).

Lemon

The moral boundaries exhibited by the carders above and the similarity they have with mainstream societal values show that the carding subculture and the mainstream culture are not distinct from one another, but draw on each other, a finding that has been identified in traditional British subcultural theory (Clarke 1974). Therefore, carders should not be seen as entirely different from law-abiding citizens, they are simply trying to achieve socially-accepted goals using alternative solutions, which in this case is carding.

***Duality***

Unlike some forms of cybercrime, such as spam and the use of malware, what Wall termed ‘true cybercrimes’ because they could not exist without networked computers (Wall 2007), carding drifts on and offline. There is a duality to it that makes it more complex (Webber and Yip 2013). Similar to Matza’s (1964) observation that juveniles drift in and out of deviant behaviour, some carders also drift in and out of cybercrime. This is observed in a thread titled “Got barred from college!!!!!”:

Well i really don't see myself carding for a living, ive been thinking about how my life would be if i had 2 paths for me to choose to follow. One would be an educated college degree life with a wife and kids or a life of carding, life of secrecy and constant fear of getting caught. The thing I’m really scared of about carding is getting prostituted in jail. LOL. ive seen those movies with a skinny guy getting prostituted in jail. That would be the lowest of lows.

Chef

---

You choose your own destiny as we all do, but I really suggest you either change your attitude or quit school or carding. It really sounds like you don’t want to live the carder lifestyle and that your just doing it as a hobby in the meantime. Carding is dampening your scholarly abilities, there’s no reason to continue unless you plan on making a living off it for a while.

You want to get a good job, you want a stable family that’s good. But you need to understand that these other activates your doing are taking away from all this. If carding is not for you, you might as well quit while your ahead. One wrong move and you’ll turn this “hobby” of yours into the only descent way to make a living, and even then it’ll be hard because your Probation Officer will be on your ass everyday. You think you can quit carding, might as well try now because soon it’ll be harder to do soon. The more you smoke it the more you need it.

Good luck with life and its many choices ….

Fink3r

---

carding should be a hobby not your life, unless you dont value your life, and love running from the LE[[22]](#footnote-22) and moving state to state

chaosm@n

T3la

As shown in the above conversation, it is evident that some cybercriminals are not full-time criminals. Rather, they have different identities on- and offline and that they drift in and out of crime (Matza 1964). Furthermore, it can be seen that some are using carding as a way to fund access to legitimate routes by, for example, using carding to finance education.

Another example of on-/offline convergence is shown in the conversation below in which a carder requested others kill another carder who was suspected of being a ripper further merging of on- and off-line experiences as a carder:

this motherfucker ripped me off for 3 laptops and 2 monitors.

i'm gonna find this motherfucker and kill him.

i hijacked his yahoo account cuz hes a fuckin idiot and i guessed his password.

his name is \*\*\*\*\* \*\*\*\*\*, and if anyone can help me put a bullet in his head, i'll give them $1,000

i believe he lives at \*\*\* \*\*\*\*\* street , in pittsburg

his girlfriends name is \*\*\*\*\* \*\*\*\*\* i believe.

i also stole his original AIM account, " \*\*\*\*\*\*\*\* "

this motherfucker is gonna get it , and get it hard. no matter what.

please believe it

As can be seen, the carder who was ripped-off had published personal details about the ripper and had requested someone kill the ripper in return for money. This shows that the real identity of a carder can sometimes be compromised, highlighting that the flexibility of their on-/off-line identities are sometimes not as separable as scholars have previously assumed, such as the “identity flexibility and dissociative anonymity” characteristic that forms a main component of Jaishankar’s “Space Transition Theory” (Jaishankar 2008). This idea suggests that it is the anonymity afforded by the Internet that encourages crime. However, evident from the conversations above, many carders operate on the assumption that they will be identified by law enforcers one day and many prepare themselves for the moment by having tools available to destroy the evidence.

Perhaps what truly differentiates carding from the more traditional form of computer hacking (Jordan and Taylor 1998; Yar 2005; Taylor 2005; Holt 2007) is how some aspects of criminality in carding necessitate interactions in real life. This duality is captured by some of the discussions in a thread called “hahaha ups guys r pussys” which was started by someone bragging about their experience with the delivery firm UPS:

dude today was awesome...me and my partner were at a drop and the ups guy was givin me shit....asking me questions cause it was an apartment complex and we were just chillin inside..anyways the ups guy came with a nice lil package...anyways he gave us problems so i took it out of his hands and pushed his ass down and got the hell out of there..it was great..what a rush

the\_drop

Although this drew the reactions from many members who saw the amusing side in the act, the more serious members saw this as a risk not worth taking:

yea way to draw attention to yourself.... seriously leave the UPS man alone, the damn guy is just doing his job.

All you did was draw attention to yourself which is the first no no in life. Then you come on here and brag about it like you deserve a cookie..

A real carder can play in smooth, hell I became friendly with the ups man back when i was a big carder... we still chill all the time, he doesnt give a fuck that i card or anything.. hes a good pal to have..You play it like your doing nothing illegal and your fine, u start beating on UPS people and taking a package and start running u look like a criminal !.. I wish a cop would have seen you so you would have some explaining to do. Then I'd like to see you brag about that one..

Sorry for the rant, but this guy isnt earning any respect with me

l33t

---

dude, listen to l33t- get in GOOD with the UPS drivers... pissing them off could mean the cops checking out that transaction NOW as opposed to in a few days when the CC comes up bad. If you get in good with the UPS driver, you are all set.

enf0rcer

The responses to this thread highlight not just the on-/off-line convergence in the crime itself but also the attitude towards risk taking. The responses show that a characteristic among carders that is much respected is *composure*, the ability to maintain control (see Lyng 1990 for a similar observation among risk-takers). Due to the criminal nature of carding and the need for offline interactions, the ability to maintain control amidst adverse conditions appears to be a particularly important skill for carders as failure to do so could well expose them to law enforcers. Therefore, whilst duality appears to be a characteristic that separates carding as a distinctive form of deviance from true cybercrimes, the importance of composure, that is, the ability to maintain control amidst adverse conditions, is a characteristic that defines a serious carder.

**Discussion and Summary**

Carding forums like ShadowCrew provide a unique methodological tool to understand carders since forum dialogue is maintained over the entire lifespan of the forum. From these dialogues, we can gain insight into those who engage in carding fraud, the discussions they have, their frailties, triumphs, and the challenges of the everyday. The focus of this chapter was on the carding subculture that emerged on ShadowCrew. In order to enhance our understanding of this carding subculture, five normative orders were examined: *networking*, *competence*, *drive*, *morality* and *duality*. The evidence presented in this chapter supports the complexity of financially motivated cybercrime and that extensive criminal networking for resources is required for sustainable profits to be made (Lusthaus 2018b). As carding involves the exploitation of technologies, extensive knowledge sharing is required and some carders have demonstrated strong commitment in mastering the crime (Leukfeldt, Kleemans, and Stol 2016c). By examining the content of a carding tutorial shared on ShadowCrew and the responses to the post, it is also clear that forums facilitate not only the social learning of the techniques of crime, but also the argots of the carding subculture, that is, the unique linguistic references used among carders which defines the subculture (Holt 2007). They are also key resources for the building and maintenance of the level of trust that is required by those engaging in risky behaviours (Yip, Webber and Shadbolt 2013) Therefore, this highlights how forums facilitate global criminal networking, a feature of financially motivated cybercrime that distinguishes it from conventional crimes (however, see Leukfeldt, Lavorgna, and Kleemans, 2017 for a discussion of the dissimilarity of cybercrime from traditional organised crime). This chapter has also challenged the mainstream stereotyping of cybercriminals and exposed their human struggle. Rather than being techno-geniuses or super-criminals, they instead engage in the same kinds of discussions that many of us who are not carders have: they worry over their choice of “career,” the ethics of what they do, and how to do the job better. Dialogues from the forum show that the carders were driven by different motives but all found carding as a common solution. This provides us with an insight into the nature of criminological theory, since many of the classical theories apply, and many overlap.

A sense of political anarchy is also observed in the discussions and in the pseudonyms they used. For some, carding was a way to “manipulate the system”, to get one over on the banks, government, and other corporations. Carding is perceived, like so much else on the Internet, as a victimless crime, or at least with little cost. Rather than the offence being against an individual, it is against the banks that will compensate the victim. In the post-credit-crunch world, where worldwide measures of austerity are weighing most heavily on those least able to bear the strain, it should be expected that cybercriminals such as hackers and carders will take on the role of anarchic, anti-establishment anti-heroes. Hacking was the prime example of innovation in the face of the seeming blocks to cherished goals, be they free telephone calls, copyright-protected games, innovative software, or money from banks without the need to work too hard. In carding, individuals appear to be Merton’s innovator, retreatist and rebel combined - a combination that demonstrates that carders cannot be explained in simplistic terms of rational choice or routine activities, or written off as just another moral panic. Many of these carders took the line that they were enriching themselves in the face of a system designed to keep everyone down, and they saw themselves as fighting the system and winning. Of course, we all actually pay for these crimes. The sense of rebellion is misplaced, and the thought that the banks are really losing out misguided. Yet, in a discussion about scamming college kids, some carders demonstrate moral values not too dissimilar to mainstream cultural values. Therefore, carders should not be portrayed as “folk devils” but people just like “us” who are also trying to accept socially accepted goals. However, the difference lies in the route they have chosen to achieve the goals. Lastly, duality, is a normative order that carding necessitates. Evidence from this forum, and elsewhere, has shown that cybercriminals drift on and off-line (Leukfeldt, Kleemans and Stol 2016a). Examples of off-line crimes associated with carding include collecting goods from drop locations and cashing out stolen bank accounts. This brings about a dimension of crime not commonly associated with cybercrime. Another aspect of being a carder is the drifting in and out of crime. Some carders on ShadowCrew had legitimate jobs in real life and found carding as a profitable “hobby”, whilst some used carding to finance education, which in other words, was using an illegitimate route to finance access to a legitimate route to a successful education.

This study also examined whether the three common traits among hacker cultures (Holt 2007), *technology*, *secrecy* and *mastery*, are also found in carding subculture. The detailed tutorial referenced in this chapter and the corresponding responses show that carders hold an intrinsic relationship with technology and there is a strong need for them to master it. However, it is unclear whether the significance of these values are as defining as those to a computer hacker subculture, or indeed a hacktivist group, mainly due to the differences in personal motivation (Webber and Yip 2018). Although many carders expressed their devotion to the thrill sensation associated with committing the crime, a testimony to their mastery, many agree that the ultimate end-goal is to make a financial profit and avoid being caught. This difference in motivation may well have an impact on the significance of mastery and technology in the carding subculture where it is often just the means to an end, rather than core values of self-identification. In other words, they are learned responses to the risks associated with the crime, and not every carder is willing or able to embed them in their carding activities (van Hardeveld, Webber and O’Hara 2017). In contrast, a hacker is defined by the skills they have, which can be employed for any number of reasons and results. In this regard, carders share more in common with hacktivists who use their knowledge to facilitate explicit results (Webber and Yip 2018).

Furthermore, although thrill is a sensation experienced by many carders, no evidence has been found which suggest that there were individuals who were seduced into carding by thrill alone. Rather, the materialistic desires caused by structural strains, as well as previous exposure to sanctions appear to be dominant factors in why individuals engaged in carding. However, this chapter argues that the role of thrill should not be dismissed entirely as it may have implications on the likelihood of a carder to reoffend after their first taste of carding and their encounter with the thrilling sensation of illicit financial gain. A closer examination into the different stages of a carder’s experience in carding is therefore proposed. Based on the responses to a forum thread that was started by a carder boasting about a physical tussle with a delivery firm, secrecy is a highly significant characteristic that is much valued in the carding subculture. This is perhaps not surprising given the inherent criminal nature of carding. However, an interesting observation from the responses to the thread is the characteristic of *composure,* which has not received much attention in cybercrime literature. Composure is a characteristic that has been shown in this chapter to be precursory to the ability to maintain secrecy, which in turn facilitates the thrill and seduction of crime. This is found to be a particularly important characteristic for carders as carding necessitates committing crimes in the off-line world. Consequently, this chapter argues that carding is a unique form of crime that is given complexity through the study of online discussion forums. Any sense that carding, indeed any crime, can be explained or prevented through a rational or routine activities perspective must also countenance the contextual, emotional and seductive qualities of risky behaviour.

**Bibliography**

Akers, R.L., (1977). *Deviant Behavior: A Social Learning Approach*. 2nd Edition. California: Wadsworth.

Akers, R.L., Krohn, M.D., Lanza-Kaduce, L., and Radosevich, M., (1979). ‘Social Learning and Deviant Behavior: A Specific Test of a General Theory’. *American Sociological Review*, 44 (4), 636–655.

Benjamin, V., Li, W., Holt, T. and Chen, H. (2015). ‘Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops’ IEEE International Conference on Intelligence and Security Informatics (ISI).

Brenner, S. (2002). ‘Organized Cybercrime ? How Cyberspace May Affect the Structure of Criminal Relationships’. *North Carolina Journal of Law & Technology*, 41 (1984), 1–50.

Clarke, M., (1974). ‘On the Concept of ‘Sub-Culture’. *The British Journal of Sociology*, 25 (4), 428–441.

Cloward, R. and Ohlin, L., (1960). *Delinquency and Opportunity*. London: Collier-Macmillan.

Cohen, A.K., (1965). ‘The sociology of the deviant act: Anomie theory and beyond’. *American Sociological Review*, 30 (1), 5–14.

Cohen, S., 2002 (1972). *Folk Devils and Moral Panics*. 3rd Edition, London: McGibbon and Kee.

Cohen, L.E. and Felson, M., 1(979). ‘Social Change and Crime Rate Trends: A Routine Activity Approach’. *American Sociological Review*, 44 (4), 588–608.

Cornish, D. B. and R. V. Clarke (1987). ‘Understanding crime displacement: An application of rational choice theory’, *Criminology* **25**(4): 933-948.

Décary-Hétu, D. and A. Leppänen (2016). ‘Criminals and signals: An assessment of criminal performance in the carding underworld.’ *Security Journal* **29**(3): 442-460.

Ferrell, J., (1999).’ Cultural Criminology’. *Annual Review of Sociology*, 25 (1), 395–418.

Ferrell, J. (2013). ‘Cultural criminology and the politics of meaning.’ Critical Criminology **21**(3): 257-271.

Glenny, M. (2011), *Dark Market: Cyberthieves, cybercops and you,* London: The Bodley Head.

Gottfredson, M.R. and Hirschi, T., (1990). *A General Theory of Crime*. Stanford: Stanford University Press.

Hall, S. and S. Winlow (2007). ‘Cultural criminology and primitive accumulation: A formal introduction for two strangers who should really become more intimate.’ *Crime, Media, Culture* **3**(1): 82-90.

Hayward, K. J. (2012). ‘Five spaces of cultural criminology.’ *The British Journal of Criminology* **52**(3): 441-462.

Hayward, K. J. (2016). ‘Cultural criminology: Script rewrites.’ *Theoretical Criminology* **20**(3): 297-321.

Hayward, K. J. and J. Young (2004). ‘Cultural criminology: Some notes on the script.’ *Theoretical Criminology* **8**(3): 259-273.

Herbert, S., (1998). ‘Police Subculture Reconsidered’. *Criminology*, 36 (2), 343–370.

Hobbs, D. (1998). ‘Going Down the Glocal: The Local Context of Organised Crime.’ *The Howard Journal of Criminal Justice* **37**(4): 407-422.

Holt, T. J. (2007). ‘Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures.’ *Deviant Behavior* **28**(2): 171-198.

Holt, T.J., 2010. Examining the Role of Technology in the Formation of Deviant Subcultures. Social Science Computer Review, 28 (4), 466–481.

Holt, T. J. (2017). ‘Identifying gaps in the research literature on illicit markets on-line.’ Global Crime 18(1): 1-10.

Holt, T.J. and Bossler, A. M., (2008), ‘Examining the applicability of lifestyle-routine activities theory for cybercrime victimization’ Deviant Behavior, 30(1), pp.1-25.

Holt, T.J., Bossler, A. M. and Seigried-Speller, K.C. (2017), Cybercrime and Digital Forensics: An Introduction, 2nd Edition, London: Routledge.

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

[Hutchinson, E.](https://www.emeraldinsight.com/author/Hutchinson%2C+Emma)(2014), ‘Researching Forums in Online Ethnography: Practice and Ethics’, in M. Hand and S. Hillyard (eds.) *Big Data? Qualitative Approaches to Digital Research (Studies in Qualitative Methodology, Volume 13)*Emerald Group Publishing Limited, pp.91 – 112

Jaishankar K., (2008).**‘**Space Transition Theory of Cyber Crimes’. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the Internet*, Upper Saddle River, NJ: Prentice Hall, pp. 283-301

Jordan, T. and Taylor, P. (1998). ‘A Sociology of Hackers’. *The Sociological Review*, 46 (4), 757–780.

Jordan, T. and Taylor, P. (2004). *Hacktivism and Cyberwars*. London: Routledge.

Kahneman, D. and A. Tversky (1979). ‘Prospect Theory: An Analysis of Decision under Risk.’ *Econometrica* 47(2): 263-291.

Katz, J., (1988). *Seductions of Crime: Moral and Sensual Attractions in Doing Evil*. US: Basic Books.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016a), ‘Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks’, *British Journal of Criminology*. 57: 2, 704-722

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016b), ‘A typology of cybercriminal networks: from low tech locals to high tech specialists’, *Crime, Law and Social Change*. 67: 1, 39-53

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016c), ‘Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis’, *Crime, Law and Social Change*, 23: 3, 287-300

Leukfeldt, E. R., Lavorgna, A. and Kleemans, E. R. (2017), ‘Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime’, European Journal on Criminal Policy and Research, Volume 23, Issue 3, pp 287–300.

Leukfeldt, E. R. and Yar, M. (2016). ‘Applying routine activity theory to cybercrime: A theoretical and empirical analysis.’ *Deviant Behavior* 37(3): 263-280.

Levi, M., (2009). ‘Suite Revenge?: The Shaping of Folk Devils and Moral Panics about White-Collar Crimes’. *British Journal of Criminology* , 49 (1 ), 48–67.

Lyng, S., (1990). ‘Edgework: A Social Psychological Analysis of Voluntary Risk Taking’. *The American Journal of Sociology*, 95 (4), 851–886.

Lusthaus, J., (2012). ‘Trust in the World of Cybercrime’. *Global Crime*, 13 (2), 71–94.

Lusthaus, J. (2018a) “Honour Among (Cyber)thieves?,” European Journal of Sociology, 59(2), pp. 191–223.

Lusthaus, J. (2018b), Industry of Anonymity: Inside the Business of Cybercrime, Cambridge, Massachusetts: Harvard University Press.

Lusthaus, J., & Varese, F. (2017), ‘Offline and local: The hidden face of cybercrime’, Policing: A Journal of Policy and Practice, pp. 1-11, Retrieved from http://doi.org/10.1093/police/pax042

Matza, D., (1964). *Delinquency and Drift*, New York: Wiley.

Matza, D. and Sykes, G.M., (1961). ‘Juvenile Delinquency and Subterranean Values’. *American Sociological Review*, 26 (5), 712–719.

McCarthy, B., (1995). ‘Not Just ‘For the thrill of it’: An instrumentalist elaboration of Katz’s explanation of sneaky thrills property crimes’. *Criminology*, 33 (4), 519–538.

Merton, R.K., (1938). ‘Social Structure and Anomie”. *American Sociological Review*, 3 (5), 672–682.

Moore, T., Clayton, R., and Anderson, R., (2009). ‘The Economics of Online Crime’. *Journal of Economic Perspectives*, 23 (3), 3–20.

Sandywell, B., (2010). ‘On the Globalisation of Crime: the Internet and New Criminality’. in Y. Jewkes and M. Yar, eds. *Handbook of Internet Crime*. Devon: Willan Publishing, 38–66.

[Sugiura, L.](https://researchportal.port.ac.uk/portal/en/persons/lisa-sugiura(52d16734-471c-40d4-94f3-94a684574741).html), Wiles, R., & Pope, C. (2017). ‘[Ethical challenges in online research: public/private perceptions](https://researchportal.port.ac.uk/portal/en/publications/ethical-challenges-in-online-research(9dc2edae-d66c-4733-b286-9f2fd30684fc).html)’. *Research Ethics*, 13 (3-4), 184-199.

Skinner, W. F. and A. M. Fream (1997). ‘A social learning theory analysis of computer crime among college students.’ *Journal of research in crime and delinquency* 34(4): 495-518.

Sutherland, E.H., (1939). *Principles of Criminology*, Chicago, IL: Lippincott.

Sykes, G.M. and Matza, D., (1957). ‘Techniques of Neutralization: A Theory of Delinquency’. *American Sociological Review*, 22 (6), 664–670.

Taylor, P. A. (1998). ‘Hackers: Cyberpunks or microserfs?’ *Information, Communication & Society*, 1 (4), 401–419.

Taylor, P.A. (2005).’ From hackers to hacktivists: speed bumps on the global superhighway?’. *New Media & Society* , 7 (5 ), 625–646.

Uzzi, B., (1997). ‘Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness’. *Administrative Science Quarterly*, 42 (1), 35–67.

van Hardeveld, G. J., Webber, C and O’Hara, K. (2017). ‘Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets.’ *American Behavioral Scientist* 61(11): 1244-1266.

Von Lampe, K., (2003). ‘Criminally Exploitable Ties: A Network Approach to Organized Crime’. In Emilio C. Viano, José Magallanes, Laurent Bidel (eds.), *Transnational Organized Crime: Myth, Power and Profit*, Durham, NC: Carolina Academic Press, 2003, pp. 9-22

Wall, D.S., (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Malden: Polity Press.

Webber, C. and J. Vass (2010). ‘Crime, film and the cybernetic imagination’. In Y. Jewkes and M. Yar. (eds), *Handbook of Internet Crime*. London, Routledge**:** 120-144.

Webber, C. and M. Yip (2012). ‘Drifting on and off-line: Humanising the cyber criminal’. In S. Winlow and R. Atkinson (eds.), *New directions in crime and deviancy*. London, Routledge**:** 191-205.

Webber, C. and Yip, M. (2018), 'The Rise of Chinese Cyberwarriors: Towards a theoretical model of online hacktivism', *International Journal of Cybercriminology,*Volume 12, Issue 1.

Wilkinson, D. and Thelwall, M. (2011). ‘Researching personal information on the public web: Methods and ethics.’ *Social Science Computer Review* 29(4): 387-401.

Winlow, S. and Hall, S. (2016), ‘Realist Criminology and its Discontents’, International Journal for Crime, Justice and Social Democracy, 5 (3): 80-94.

Yar, M., (2005). ‘Computer Hacking: Just Another Case of Juvenile Delinquency?’, *The Howard Journal of Criminal Justice*, 44 (4), 387–399.

Yip, M., Shadbolt, N., & Webber, C. (2013), ‘Why forums? An Empirical Analysis into the Facilitating Factors of Carding Forums’, Paper presented at ACM Web Science 2013, France.

Yip, M., Webber, C., & Shadbolt, N. (2013), ‘Trust among cybercriminals? Carding forums, uncertainty and implications for policing’, Policing and Society, 23(4), 516-539.

1. At the end of each forum post the poster’s pseudonym appears, we have not changed these names since the forum posts that we use here were publically available and several of the forum posters have been discussed elsewhere (see eg. Lusthaus 2018b for a discussion on the history of ShadowCrew). [↑](#footnote-ref-1)
2. Jonathan Lusthaus (2018) has written a timely study that provides a nuanced perspective of cybercrime, drawing on one of cultural criminology’s key inspirations, Jack Katz’s (1988) *Seduction of Crime.* Nevertheless, routine activity theory still forms the core theoretical narrative of the book. [↑](#footnote-ref-2)
3. Slang for Fed or the Federal Bureau of Investigation, FBI [↑](#footnote-ref-3)
4. Credit card, also CCz, or ccz, for plural [↑](#footnote-ref-4)
5. Slang for anyone who is new to the site or to carding. Alternatives are ‘newbie’, or similar. [↑](#footnote-ref-5)
6. A system to allow anonymous internet relay chats, the underlying software that enables discussion forums. [↑](#footnote-ref-6)
7. refers to "web shells", scripts placed on to a server that would provide an attacker with remote access to the server's operating system. [↑](#footnote-ref-7)
8. refer to having root user privilege which provides the user with unrestricted access to files on the system. [↑](#footnote-ref-8)
9. Shadowcrew [↑](#footnote-ref-9)
10. see Lusthaus 2012 for more on this. [↑](#footnote-ref-10)
11. addresses [↑](#footnote-ref-11)
12. [↑](#footnote-ref-12)
13. [↑](#footnote-ref-13)
14. These abbreviations are all explained below [↑](#footnote-ref-14)
15. proxies - refers to a proxy, a server designed to  receive and relay network traffic to the intended server. [↑](#footnote-ref-15)
16. Wingate is a particular server application to set up a Windows server as a proxy server. [↑](#footnote-ref-16)
17. SOCKS is an authenticated proxy server with the ability to relay network traffic of various protocols including Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP). [↑](#footnote-ref-17)
18. We have changed the name of the programme for this chapter [↑](#footnote-ref-18)
19. HD refers to hard drive or hard disk. [↑](#footnote-ref-19)
20. This is Shadowcrew’s motto and appears at the top of the website page. [↑](#footnote-ref-20)
21. 1000 [↑](#footnote-ref-21)
22. Law Enforcement [↑](#footnote-ref-22)