ABSTRACT
Over the last decade, the nature of cybercrime has transformed from naive vandalism to profit-driven, leading to the emergence of a global underground economy. A noticeable trend which has surfaced in this economy is the repeated use of forums to operate online stolen data markets. Using interaction data from three prominent carding forums: Shadowcrew, Cardersmarket and Darkmarket, this study sets out to understand why forums are repeatedly chosen to operate online stolen data markets despite numerous successful infiltrations by law enforcement in the past. Drawing on theories from criminology, social psychology, economics and network science, this study has identified four fundamental socio-economic mechanisms offered by carding forums: (1) formal control and coordination; (2) social networking; (3) identity uncertainty mitigation; (4) quality uncertainty mitigation. Together, they give rise to a sophisticated underground market regulatory system that facilitates underground trading over the Internet and thus drives the expansion of the underground economy.

Author Keywords
cybercrime; carding; underground economy; social computing; web 2.0

ACM Classification Keywords
H.2.8 [Database Management]: Database Applications – Data Mining; K.4.2 [Computers and Society]: Abuse and crime involving computers

General Terms
Security, Human Factors, Theory.

INTRODUCTION
Despite over a decade of extensive research into computer and cyber security, cybercrime remains one of the primary threats facing governments, corporations and ordinary citizens [31]. This raises an intriguing question: how has cybercrime managed to evolve into the persistent problem we are facing today?

One of the main reasons is the emergence of a profit-driven underground economy [10, 18, 31] in which cybercriminals with a variety of different skills and resources trade competitively according to the laws of market supply and demand. One major source of profit driving this underground economy is carding: a type of identity theft which involves the unauthorised use of credit and debit card account information to fraudulently purchase goods and services [21]. The scope of the term has evolved over the past few years to incorporate a broader range of related activities including hacking, phishing and auction frauds.

![Figure 1: The Underground Economy.](image)

Labour specialisation has emerged in this sophisticated “underground economy” (see fig. 1) with key roles including carders, hackers, malware authors, phishers and spammers. As Moore et al note [18]:

Just as in Adam Smith’s pin factory, specialization has led to impressive productivity gains, even though the subject is now bank card PINs rather than metal ones.

However, there also exists dishonest traders among cybercriminals, known as the “rippers”. These rippers take advantage of the anonymity of the Internet and trade
dishonestly, stealing money from cybercriminals. In essence, they erode the trust in the underground economy and thus increasing the uncertainty among cybercriminals. To avoid this ripper “tax”, many carders have formed closed knit carding forums in the form of closed membership carding forums [10]. A snapshot of one of the earliest carding forums called Shadowcrew is shown in fig. 2. Members of Shadowcrew are believed to have trafficked at least 1.7 million credit cards and inflicted more than 4 million dollars worth of damage [5]. Many carding forums have since appeared including Carderplanet [8], Cardersmarket [22], Darkmarket [8] and Ghostmarket [15].

The implications of this study is to help security practitioners better understand the socio-economic requirements of online underground trading among cybercriminals so that they can better estimate the size of the underground economy, its scalability and scanning the horizon for new web applications which may be used to facilitate online underground trading.

MOTIVATION AND RELATED WORK
One of the first to publish on the functioning of the underground economy are Thomas and Martin [25] who revealed the process of illicit trading of stolen credit card data over the Internet Relay Chat (IRC). Franklin et al performed a detailed statistical analysis of the carding merchandise traded on the IRC [6]. There are also three recent studies on underground forums. Holt and Lampke [12] manually analysed six forums and found that the dynamics of the stolen data markets are governed by four key factors: communications, price, quality and service. Lusthaus [15] analysed the structure of online criminal groups through the use of interviews with hackers and data from a carding forum named Ghostmarket. Lastly, Mutoyama et al [19] analysed six underground forums with one German carding forum called carders.cc. However, like previous studies on carding activities on the IRC, this study focuses on the statistical analysis of the forum.

The study presented in this paper differs from the above by investigating the socio-economic requirements of online underground trading and how they are facilitated by carding forums.

DATASET: CARDING FORUMS
Shadowcrew was founded in 2002 by Andrew Mantovani, a 20 year-old part time business student in Arizona. He was already a member of a hacking group at the time but one which only stored stolen data [9]. He realised that there was a need for a place to trade stolen data online and after meeting David Appleyard, a mortgage broker in his 40s, they founded one of the earliest carding forums: Shadowcrew. When it was finally shut down in 2004 as part of Operation Firewall [5, 8, 22], Shadowcrew members had already trafficked more than 1.7 million credit card numbers and inflicted over 4 million dollars worth of damage. The same operation also led to the demise of another significant but Russian speaking carding forum called Carderplanet which began operation in 2001[8, 22].

In order to fill the void left behind by Carderplanet and Shadowcrew, two carding forums emerged in 2005: Cardersmarket and Darkmarket [8, 22]. Both forums were engaged in a bitter board war over the course of their co-existence until being taken down in 2007 and 2008 respectively, [8, 22]. This highlights the value of carding forums in the underground economy and thus warrants an investigation into why forums are repeatedly chosen to operate online stolen data markets.

A crucial question which has thus far received little attention from security researchers is why are forums repeatedly chosen to operate online stolen data markets despite numerous successful infiltrations by law enforcement? This is the question addressed in this study.

In collaboration with the Serious Organised Crime Agency (SOCA), this project has been granted access to the anonymised interaction data from two high profile carding forums which were recently taken down [8, 22] Cardersmarket (CM) and Darkmarket (DM). Furthermore, we have access to the qualitative archive of a snapshot of Shadowcrew (SC) which provides us with a unique set of qualitative data to supplement our statistical analysis.

Drawing on theories from criminology, social psychology, economics and network science as well as using a unique set of quantitative and qualitative data available, the aim of this study is to investigate the reasons for forums to be repeatedly chosen by cybercriminals to operate online stolen data markets. From our analysis, we find that there are four crucial socio-economic mechanisms offered by the forums and which together greatly facilitate online underground trading:

- Formal control and coordination
- Social networking
- Identity uncertainty mitigation
- Quality uncertainty mitigation

Figure 2: Interface of Shadowcrew.
Much like conventional online discussion forums, carding forums are used mainly for trading carding goods and services. A carding forum is typically divided into a series of sub-forums each dedicated to a particular type of content such as trading, tutorials, discussions and a blacklist of dishonest traders (the “rippers”). Users can start topics, also known as threads, which others can reply to by creating posts. Members can also communicate via private messaging (PM) which is often used by carders to carry out more detailed negotiations. Members are free to network with one another to engage in discussions and trading. Potential trading partners could either contact each other via private messaging on the forums or other means of contact such as email or ICQ. In this study, we have access to the anonymised interaction data from Cardersmarket (CM) and Darkmarket (DM), as well as a qualitative archive of a snapshot of Shadowcrew (SC). The CM and DM datasets are summarised in table 1.

The following section presents an empirical analysis into the facilitating mechanisms offered by carding forums.

**ANALYSIS**

Previous studies have observed underground trading activities on both the IRC [6, 25] and forums [12, 15, 19]. However, using the ”market for lemons” theory from economics, Herley and Florêncio [10] argue that the prevalence of dishonest traders (a.k.a. "rippers") in the underground economy means there is too much uncertainty for a competitive market to emerge on open platforms like the IRC. Rather, the majority of serious trading occur in closed gangs such as carding forums. This study builds on this claim by proposing four socio-economic mechanisms offered by carding forums which together greatly facilitate underground trading over an anonymised environment such as the Internet and thus explain why forums are repeatedly chosen by cybercriminals to operate online stolen data markets.

- **Formal control and coordination:** according to Transaction Cost Economics (TCE), a hierarchical structure has lower coordination costs than a pure market structure and thus more suitable for organisations with high coordination requirements [23, 29]. Since by its nature the underground economy involves dishonest individuals, coordination activities such as membership administration is paramount to the emergence of a competitive stolen data market. We hypothesise that the inherent hierarchical management structure and network boundary offered by forums greatly assists cybercriminals in implementing a well coordinated management system for monitoring and regulating behaviour in the underground market.

- **Social networking:** trading is a social activity as it requires one to interact with others. Therefore, essential to the success of a cybercriminal is to network with fellow cybercriminals in order to find the appropriate supplies and demands as well as opportunities. Akin to the legitimate world, social capital [2] is significant to the success of a cybercriminal. In the criminal world, this translates to criminal capital [16] which includes access to skills, resources and information for criminal purposes. We therefore hypothesise that carding forums are repeatedly chosen as they facilitate social networking among cybercriminals.

- **Identity uncertainty mitigation:** due to the anonymity offered by the Internet, it is difficult for the cybercriminals to determine whether a potential trading partner is a serious cybercriminal, a potential ripper or a law enforcement associate. It is important to note that it was the latter which helped bring down Shadowcrew [5, 8]. As outlined in [4, 7, 26], the knowledge of a person’s past is vital to the emergence of trust. Due to the asynchronous nature of forum contents, carding forums allow cybercriminals to monitor the past behaviour of one another. Unless explicitly removed by those in charge, forum contents such as threads, posts and private messages are archived over time. Therefore, if one needs to decide whether a potential trader is trustworthy, they could perform a search for the person’s past record of interactions with the community to see if there has been any unusual behaviour which may appear deviant from the community’s norms [11, 28]. Therefore, we hypothesise that carding forums allow cybercriminals to mitigate identity uncertainty by facilitating the development of in-group identity and prototypical behaviour through repeated symbolic interactions with one another [24, 30].

- **Quality uncertainty mitigation:** as already mentioned, one of the major obstacles for cybercriminals to trade over the Internet is the prevalence of rippers. As described by Herley and Florêncio [10], these rippers trade dishonestly using a variety of methods such as double selling the same set of stolen credit card data to multiple buyers. Therefore, for the serious cybercriminals, there is a great amount of uncertainty about the quality of goods and services offered by the vendors with whom they may not have prior trading.

<table>
<thead>
<tr>
<th>Forum</th>
<th>Operational Period</th>
<th>Users</th>
<th>Threads</th>
<th>Posts</th>
<th>PMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM</td>
<td>2005 - 2007</td>
<td>2759</td>
<td>7476</td>
<td>31391</td>
<td>24836</td>
</tr>
<tr>
<td>DM</td>
<td>2005 - 2008</td>
<td>2075</td>
<td>6240</td>
<td>32089</td>
<td>15370</td>
</tr>
</tbody>
</table>

Table 1: Summary statistics of Cardersmarket (CM) and Darkmarket (DM).
experience. We hypothesise that forums mitigate this uncertainty by offering a comprehensive review process for prospective vendors which is enforced by the hierarchical management structure.

Together, the above four socio-economic mechanisms give rise to a sophisticated underground market regulatory system as shown in fig. 3. The following present the empirical evidence which verifies our hypothesis outlined above.

**Formal control and coordination**

One of the most distinctive characteristics of forums is the inherent hierarchical management system, which is shown in fig. 4. Below is a brief description of the common ranks assigned to registered users on carding forums. It is particularly important to understand the roles as they are vital to the socio-economic mechanisms shown in fig. 3.

**Administrators:** they are responsible for the overall management of the forum and making long term strategic decisions. Such strategic decisions include protecting the forum from attacks by other similar carding forums, should they become involved in a “board war” [8, 22]. Administrators are also responsible for managing the forum members including rewards and punishments when appropriate. In particular, they safeguard the forum by removing the “rippers”, the members who have cheated money off others.

**Moderators:** the moderators are responsible for the management of the sub-forums which either fall into their expertise or geographical location. They specify the rules for posts as well as removing inappropriate ones.

**Reviewers:** their duty is to test illicit goods and services from the members wishing to become a vendor. This is the key part of the trust mechanism in place as these few reviewers are endorsed by the majority as trustworthy and the trust on them propagates to the vendors they review, allowing quality assurance to take place and propagate as supply increases.

**Reviewed vendors:** they are those who have been referenced by the reviewers and are deemed as trustworthy. As reputation is crucial to their success and since the only way the system could recognize these reviewed vendors is through their chosen username, the usernames become attached to their reputation. Thus, most members rarely change their usernames within a forum [15].

**Members:** normal members who are not reviewed vendors may also sell goods on carding forums but they most often sell at lower prices due to the lack of reputation. Those who buy from them bare the risk at their own discretion. The services offered by the members are generally similar to the ones listed by Thomas and Martin [25] and Franklin et al [6]. Many carders are members of multiple forums [8, 22].

Having understood the roles of each rank, it is appropriate to examine how this hierarchical management structure enables formal control over the forum members. This is best demonstrated using a combination of qualitative quantitative data. Below is a complaint against a potential ripper posted on a carding forum:

> Earlier today Hacker666 made a post looking for pin cashers. Like many members I jumped on this and messaged him. He will try to get you to send money to his E-gold account before cashing. This is to make sure you are not a ripper. So I get suckered and send him $250 his cut on something that was supposed to pull $500. I sent the e-gold and he removes me from his
contact list and ignores me LOL. I deserve to lose that cash, I was foolish.. greed got the best of me. Be smarter than me and no one else make this mistake. Oh and other thing he does is jerk you around for hours. He jerked me around for hours and hours before telling me to send the E-gold.

Ok, Looks like the gods have spoken. I see hes been banned. I dont know if that was before me or not. Anyway this post is a moot point now, I dont know if anyone else was taken though.

This extract represents a typical complaint against dishonest traders on carding forums. As shown, the administrators saw the complaint and the ripper was subsequently banned. However, it appears that only administrators are allowed to ban members, as shown in the following extract from a moderator’s response to a ripper complaint:

He is dropped from the vendor list. I can't ban him outright since I'm not an admin, but that wouldn't do any good anyways. You guys with information on him need to apply some pressure - maybe PM Hacker123 about this?

This highlights the power delegation and coordination between those on the management hierarchy. Evidently, the inherent hierarchical management structure of forums lowers the cost of implementing an effective regulatory system on forum activities. Furthermore, this hierarchical approach allows the management team to react quickly to problems. As shown in the extract, a member lodged an unverified complaint about a vendor being a potential ripper. However, since verification takes time and banning requires the administrator’s authorisation, the moderators immediately took action to mitigate the problem by removing the vendor from the vendor list. This demonstrates a high level of coordination in management [23, 29].

Lastly, it is interesting to observe that rippers are problematic even on carding forums. As shown in fig. 5, the arrival time of each new user registration is binned together by the number of months since the earliest registered user. The most striking pattern observable from the figure is that both forums experienced an identical sudden decay of new user registrations and signups remained extremely scarce until their eventual demise. A manual examination of the confidential qualitative data from the two forums revealed that the administrators from both forums decided to disable membership in order to keep rippers from returning to the forums using different nicknames and email addresses. This highlights the scale of dishonest trading in the underground economy and the importance of the network boundary offered by forums as it allows the segregation of dishonest behaviour from the market.

**Social networking**

As already mentioned, social networking is vital to the success of cybercriminals as it allows them to gain access to social capital [2] such as resources and opportunities which they do not otherwise possess. In order to verify our hypothesis that carding forums facilitate the social networking among cybercriminals, we set out to examine whether carding forums exhibit two well known social network properties: preferential attachment [1] and small-world phenomenon [27].

In order to examine the two network properties, we focus on the private message (PM) interactions among cybercriminals as they are used to discuss details of
The data is also modelled as an undirected graph \( UG \) where \( UG = \langle V, E \rangle \) with \( E = \{ e_1, e_2, \ldots, e_n \} \) where \( E \) is an ordered set of weighted undirected edges formed by combining the weights from reciprocal arcs. This is necessary for measuring the diameter (D) and clustering (C) of the PM graphs. The social graphs are summarised in table 2.

<table>
<thead>
<tr>
<th>Number of vertices</th>
<th>CM</th>
<th>DM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max out-degree</td>
<td>257</td>
<td>791</td>
</tr>
<tr>
<td>Max in-degree</td>
<td>128</td>
<td>196</td>
</tr>
<tr>
<td>Median out-degree</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Median in-degree</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Max degree</td>
<td>275</td>
<td>840</td>
</tr>
<tr>
<td>Median degree</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Density</td>
<td>( 4 \times 10^{-3} )</td>
<td>( 5 \times 10^{-3} )</td>
</tr>
</tbody>
</table>

Table 2: Summary statistics of the PM social networks.

<table>
<thead>
<tr>
<th>Number of arcs</th>
<th>CM</th>
<th>DM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max out-degree</td>
<td>9465</td>
<td>7545</td>
</tr>
<tr>
<td>Max in-degree</td>
<td>11749</td>
<td>10154</td>
</tr>
<tr>
<td>Median out-degree</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Median in-degree</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Max degree</td>
<td>275</td>
<td>840</td>
</tr>
<tr>
<td>Median degree</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Density</td>
<td>( 4 \times 10^{-3} )</td>
<td>( 5 \times 10^{-3} )</td>
</tr>
</tbody>
</table>

Table 3: The network diameter (D) and clustering coefficient (C) of the undirected PM graphs and their Erdős-Rényi (ER) equivalent. Each ER graph was identical in size with the relevant PM graph and the edge creation probability was set to the density of the PM graph.

### Preferential attachment

First proposed by Barabási and Albert [1], the degree distribution of many social networks have since been found to follow a power law distribution [1, 3]. One of the most common explanations for a power law degree distribution is the “the rich get richer” effect, better known as preferential attachment.

As shown in fig. 6, neither the in- nor out-degree distributions of the PM graphs follow a power law decay. Rather, they are best approximated by a lognormal distribution, a distribution cousin to power law [3, 13, 20]. This indicates that non-linear preferential attachment exists on the forums and that a fraction of the PM relations were established randomly [13, 20]. In other words, although some forum members interact with others with a specific preference (e.g. reputation), some do interact without preference, perhaps for finding new business opportunities in the wild.

Furthermore, studies [3, 20] argue that lognormal degree distribution is in fact more common than first thought and they are often misinterpreted as power law distributions. Therefore, since similar behavioural patterns have been observed in a variety of social networks [3, 13, 20], we believe our findings indicate that carding forums do facilitate social networking among cybercriminals.

### Small World

The small world phenomenon also has important implications for the underground economy because as demonstrated by Kleinberg [14], a small world greatly enhances the navigation within a social network. Shortcuts exist in a small world that enables any pair of vertices in the network to connect with one another through a relatively small number of hops. This suggests that if the carding forums are capable of producing small worlds then they are capable of producing shortcuts in the underground economy and hence bringing cybercriminals closer together. In other words, if carding forums give rise to small worlds then our hypothesis would be proven correct.

Watts and Strogatz [27] found that small world social networks commonly exhibit two network properties: path lengths as short as that exhibited by a random lattice (such as an Erdős-Rényi graph) but with a much higher degree of clustering than random structures. The network diameter D and clustering coefficient C of the two PM social networks and their Erdős-Rényi (ER) counterparts are shown in table 3.

Evidently, both social networks exhibit a clustering coefficient an order of magnitude greater than their random counterpart whilst their path lengths remain identically small relative to the network size. Therefore, our findings support our hypothesis that carding forums facilitate social networking among cybercriminals and thus are capable of giving them access to criminal capitals which they otherwise would not possess.
Identity uncertainty mitigation
By offering a space for cybercriminals to engage in reciprocal and mutually beneficial acts such as the exchange of valuable information, these are the symbolic interactions through which in-group identity and group classification can be developed [24]. This allows the members to develop an understanding of the prototypical characteristics of the group and this implicitly gives them the ability to identify those who do not belong to the group. In other words, social networking facilitates the emergence of informal social control in the underground economy.

An example of such interaction is shown in the following forum extract below:

Hacker123: People who’s life is carding and other type of frauds (so no fucking students who do this part-time);
Do you sometimes wish you just had a normal life, with this I mean normal job, no stress about ops, making money, Law Enforcement etc?
or are you 100% happy with ur ’underground ops life’ ?
I would appreciate any input/thoughts

-----

Whatever123: I wish I had a normal life. Turn back the clock and all, but fuck it I am where I am.

-----

Yeah123: Some parts of it I love. I’m a total loaner outsider, some by choice and some by the fact I’ve never been the type of guys 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 to. I hate that part of it. I’m never going to have a normal life even if I try, so this life, as ********* says, “For those who wish to play in the shadows” I love the shadows. I love doing things in the shadows. That’s where I’m comfortable.

The last post by Yeah123 is of particular interest as it shows a rare and unique glimpse of the fragile side of a cybercriminal [28].

In order to verify our hypothesis that participation in social networking facilitates trust building among cybercriminals, we examined the impact of thread and post degree have on PM degree. The results are shown in fig. 7-9. All regression models presented have a p-value ≤ 0.05 and the estimated parameters α and β represent the gradient and y-intercept of the linear regression line $y = αx + β$ respectively.

As shown in fig. 7, we found a strong positive correlation between threads/posts degree and PM degree. However, this is not enough to verify our hypothesis as this could just imply that users active in public discussions are also active in private messaging. Therefore, we also examined the relationship between thread/post degree and the number of initial contacts received via PM. As shown in fig. 8, we found a strong positive correlation between thread degree and the number of initial contacts received via PM. We also found a positive correlation between post and initial contacts received via PM, albeit a weaker correlation than that with threads. This indicates that participation in public discussions do increase the number of incoming private contact from other forum members, in particular, through the creation of new threads.

Lastly, we examined the relationship between the number of common threads shared among any two users and the number of PMs exchanged. As shown in fig. 9, we found a significant positive correlation between the two on CM which indicates that sharing common threads leads to higher levels of intimacy. However, the same relationship appears negligible on DM although the low $R^2$ score suggests a poor fit due to noisy data.

Nevertheless, we can conclude that the findings presented in this section support our hypothesis on the effects of social networking and the development of trust.

Quality uncertainty mitigation
As Gambetta [7] notes:

In stable markets, in which agents can plausibly contemplate being in business for long periods of time
and in which information travels well, the best way to establish one’s reputation for trustworthiness is simple: behave well and live up to one’s promises just as dealers do in many ordinary businesses.

Like in the legitimate business world, reputation is key to a cybercriminal who strives to profit from their criminal endeavour. However, it is useful to realise why reputation is needed in the first place. It is needed because many who want to collaborate have no prior knowledge or experience with the other. Accumulating a reputation by behaving well over time is difficult and time consuming as many simply refuse to deal with those without a reputation in the first place. Therefore, there must be mechanisms to bootstrap initial trust among cybercriminals who have not collaborated with one another before [17, 26]. One such mechanism offered by carding forums is review. A prospective vendor can offer to have their goods and/or services reviewed by an approved reviewer on the forum. A successful review will result in the vendor gaining the title: “Reviewed Vendor” – an approval of quality.

In order to examine the effect of this seal of approval, we compared the network statistics of the reviewed vendors against those who are on trial or unreviewed. As shown in table 4, there is a surprisingly few number of vendors on both forums. One explanation is that there are very few who...
In general, reviewed vendors have a much higher median PM degree regardless of direction, almost doubling that of the unreviewed vendors. Similarly, reviewed vendors on both forums are far more active on public discussions with twice as many posts created and at least three times as many posts. Furthermore, the reviewed vendors receive and initiate almost twice as many initial contacts via PM. Altogether, the findings indicate that reviewed vendors are more active than those who are unreviewed. The fact that the reviewed vendors receive twice as many initial contacts demonstrates a higher level of trust shown towards them, thus supporting our hypothesis that carding forums mitigate quality uncertainty.

It is also interesting to observe that the median in- and out-degree of the neighbouring vertices (with whom they have exchanged at least one PM) are generally higher for unreviewed vendors. One explanation is that they tend to communicate with more established members whom have accumulated higher PM degrees than themselves. Perhaps this is due to the fact that the more established members are more willing to take risks as they have more experience. On the other hand, reviewed vendors have a lower neighbouring degree which suggests that they tend to communicate with the less established members. This further supports our hypothesis that quality uncertainty is mitigated by the review process offered by carding forums.

Finally, it is important to note that this uncertainty mitigation mechanism is enforced by the regulatory system shown in Fig. 3 so that any vendor, regardless of whether they are reviewed or unreviewed, would be punished if they were found to have traded dishonestly.

**CONCLUSION**

Using interaction data from three well known carding forums previously in operation over the Internet, this study has examined why forums are repeatedly chosen to operate online stolen data markets. Our findings indicate that carding forums provide four fundamental socio-economic mechanisms which greatly facilitate underground trading over the Internet. They are: (1) formal control and coordination; (2) social networking; (3) identity uncertainty mitigation; (4) quality uncertainty mitigation. Furthermore, we have shown that the four mechanisms supplement one another, giving rise to a sophisticated underground market regulatory system. This demonstrates the robustness of carding forums and explains why they are favoured by cybercriminals. The findings from this study will allow law enforcement and security practitioners to better understand the nature and estimate the scale of the underground economy. The findings will also be useful for scanning the horizon for new applications which offer similar mechanisms and hence may be misused in similar ways to forums.

**ACKNOWLEDGMENTS**

We thank the Serious Organised Crime Agency (SOCA) from the U.K. for their support throughout this project. This research was funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, EP/G036926/1.

**REFERENCES**


