Inside Online Carding Courses Designed for Cybercriminals

Card fraud more sophisticated than ever, and what you can do about it

digital shadows_

Executive Summary

Payment card fraud costs banks and merchants billions every year. As consumers spend more and more money online, the opportunities for fraud increase; experts project a loss of $24 billion to payment card fraud by the end of 2018.[1] Payment card fraudsters do not operate in a vacuum, instead relying on a sophisticated ecosystem and support network that provides a wide range of credit card details, fraud tools and online tutorials. This paper looks at one recent online course designed for bad actors in order to shed light on the latest fraud tactics and tools, allowing consumers, merchants and credit card companies to better understand the threat and make it harder for the fraudsters.

Table of Contents

Payment card fraud is big business – and it's getting even bigger

Payment card fraud has been around as long as the cards themselves, and there are two main approaches: physical card fraud and Card Not Present (CNP) fraud. Physical card fraud entails the cloning of payment cards, which are then used to make purchases. Despite its imperfections, recent research indicates that the increasing adoption of EMV has made physical card fraud more difficult, making CNP fraud more popular.[2] CNP fraud occurs when the customer doesn't physically present the card and uses card details online or over the phone.

With consumers spending more and more with their credit cards online, it's easy to see why CNP fraud is big business. One recent report claims that annual online card spending will double to $6 trillion by 2021.[3] All of this offers more opportunities for cybercriminals to make money. This year, Europol coordinated an effort to disrupt an organized crime group that affected more than 130,000 payment cards, resulting in a loss of 8 million Euros. The criminal network established several fake online shops and a shell software company, allowing them to make illicit credit card transactions.[4] This is just one technique used by carders; cybercriminals are continuously innovating and devising new techniques to bypass security controls developed by credit card companies and merchants. The combination of increased spending and criminal innovation contributes to a projected loss of $24 billion to credit card fraud in 2018.[5]

$24 Billion

Projected loss to credit card fraud in 2018

Where do the carders learn and hone their skills? Well, just as consumers use online courses, so do cybercriminals. In order to understand carders' latest tactics and tools, we are highlighting an online course from an exclusive Russian carding forum, complete with webinars, instructors and reading material. While tutorials and guides have existed for many years, the online course was on a scale and level of professionalism we have not seen before. We will glean insights from this course so that you can understand the carding ecosystem and the latest techniques used by cyber criminals. In doing so, you as a defender can learn what makes an attractive target, and what causes problems for cybercriminals. This is relevant for financial services organizations; but there are also implications for consumers, e-commerce, hotels, airlines, gaming and retail companies. As this paper will show, carding guides and courses are not a new phenomenon, but the professionalism, reputation and freshness of this course provides useful insights for organizations across a range of industries as well as consumers.

Fraudsters are only one part of a broader ecosystem

Payment card fraudsters rarely operate by themselves, instead relying on a well-established ecosystem that provides them with payment card information, support services and ways to monetize the fraud. We have identified four key pillars of the carding ecosystem.

1. Payment Card Data Harvesters

'Harvesters' do the 'dirty work' in terms of harvesting payment card information. This is done through intercepting card holders' information whether this be through point of sale malware, skimming devices, phishing, breached databases, or through operating botnets. With the control of botnets, criminals can gain access to individuals' computers and steal their credit card information. In one recent case, a Russian criminal was sentenced to nine years in prison for operating several botnets that were used to steal credit card information. He claimed to have acquired 40,000 credit card details through this technique.[6] Criminals who amass large amounts of fresh card details can quickly and easily sell these on to distributers and make good money. In the world of Netflix's drama, *Narcos*, these would be the criminals making the goods.

2. Distributors

Distributors are the 'middle men' who typically make the most money. While the criminals who harvest may use the card data themselves, they also sell it on to others who will package, repackage and sell the card information. This may be done privately or through specific sites that sell the card details, sites that Europol refers to as Automated Vending Carts (AVCs). Seleznev – also known as nCuz, Bulba and Track2 – was a prolific Russian cybercriminal and credit card thief, responsible for 3,700 financial institutions losing more than $169 million.[7] Roman Seleznev ran many AVCs before being sentenced to 27 years in prison in April 2017. Criminals running AVCs have the potential to make a large amount of money with a low degree of risk. If the harvesters are the Narcos, the AVC owners are the distributors; reselling the product and taking their cut.

3. Payment Card Fraudsters

Fraudsters are the 'users' who actually carry out the fraud, using card details to carry out fraudulent transactions to buy goods and services. These individuals run the most risk in terms of getting caught by law enforcement or being conned by fellow criminals. Once fraudsters have acquired payment card information from their distributor, the fraud can happen. These individuals tend to be less technical and attract a lower caliber of cybercriminal, often relying on online guides and courses to learn the latest techniques. There are many approaches to this, but it typically starts by purchasing online goods for consumption or resale. The fraudsters either keep the ill-gotten goods for themselves, or they are monetized by offering the same good for a much-reduced price, such as a luxury watch for 50% off. With the right knowledge and approach, fraudsters have the opportunity to make a significant amount of money, although the risk is higher. They are the ones who make the Narcos rich and fuel the industry; if they weren't buying credit card details, the demand to drive harvest and distribution would be reduced.

4. Monetization

There are many different roles within this stage, including those who have been duped into operating drop addresses and those involved in the reselling of fraudulently acquired goods. Purchasing goods with stolen payment cards can be useful, but the payment card fraudsters will need individuals to help them monetize (cash out) these fraudulent purchases. Cashing out is necessary in order to turn carding into a business. Those involved in the cashing-out process are not always aware they are committing a criminal act; a common approach is to have unwitting individuals working for a fictitious organization, reshipping fraudulently-purchased goods as a "Merchandise Manager" or "Junior Packing Coordinator."[8]

These four areas are not mutually exclusive – a criminal might harvest the card data and commit the fraud. However, the maturity of the carding ecosystem allows actors to become more specialized. Although carding is comprised of these four key pillars, they also rely on many support services including network anonymity providers and reputation services. A great example of this specialization is fraud[.]cat, a service that allows fraudsters to determine the risk of using particular IP addresses (Figure 1).

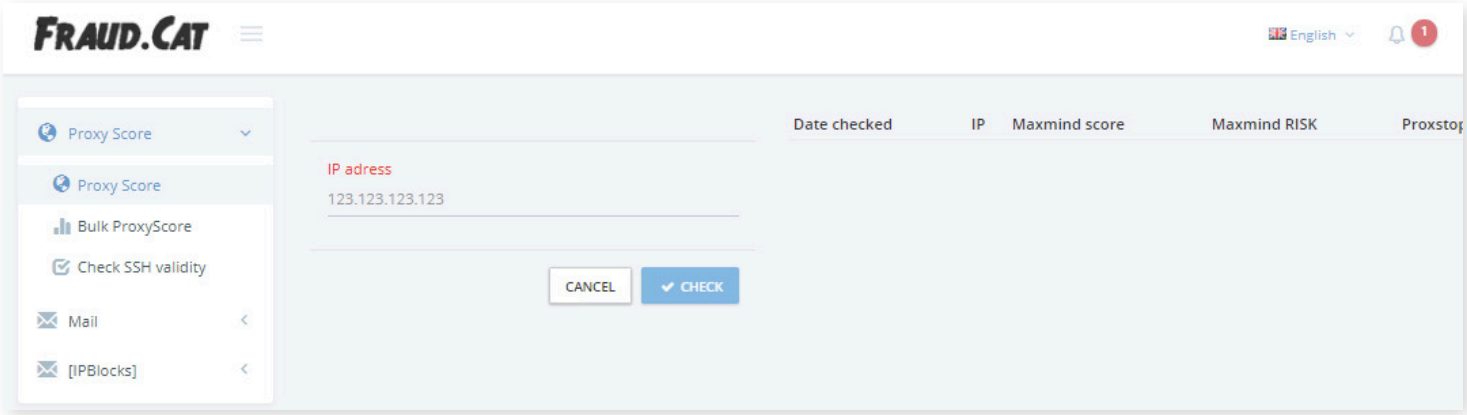


Figure 1: A screenshot of fraud[.]cat, an online service to check the risk score of IP addresses that are used for committing fraud

The online course we will cover in this paper focuses on the payment card fraudsters across the three main stages:

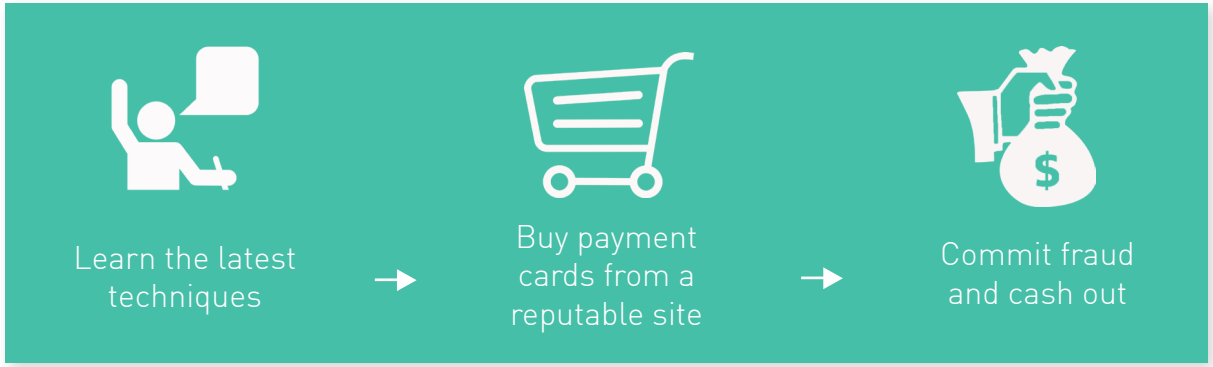


Figure 2: The 3-stage process for payment card fraudsters

By understanding what causes these criminals friction at each stage, organizations and consumers can deter these low-level criminals.

Stage 1: Learn the latest techniques

For budding cybercriminals looking to learn the latest techniques, there are many resources they can turn to. Aside from getting advice from forum peers, individuals can buy guides offered for sale on marketplaces. All carding guides aren't created equal; there is a range in quality of the guides. The better guides will have less well-known and more recent tips and, therefore, command a higher price. Figure 3 is an example of the guides at the lower end of the price range, available for only $1.

At the other end of the spectrum from a carding guide, is an exclusive online course. Digital Shadows has studied an intensive 6-week online carding course that is designed to take a novice and turn them into a specialist. The aim of the course, as shown in Figure 4, is to teach individuals "to become a professional in the world of carding." The cost of the course is 45,000 RUB ($745), with an additional $200 to be paid for course materials, payable with e-currencies such as Webmoney or Bitcoin. Unlike the ubiquitous $1 guides available on marketplaces, this is not a self-paced, generic tutorial.

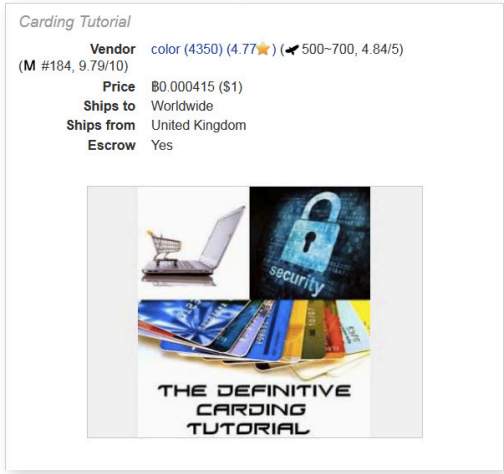


Figure 3: A $1 carding guide offered on a dark web marketplace

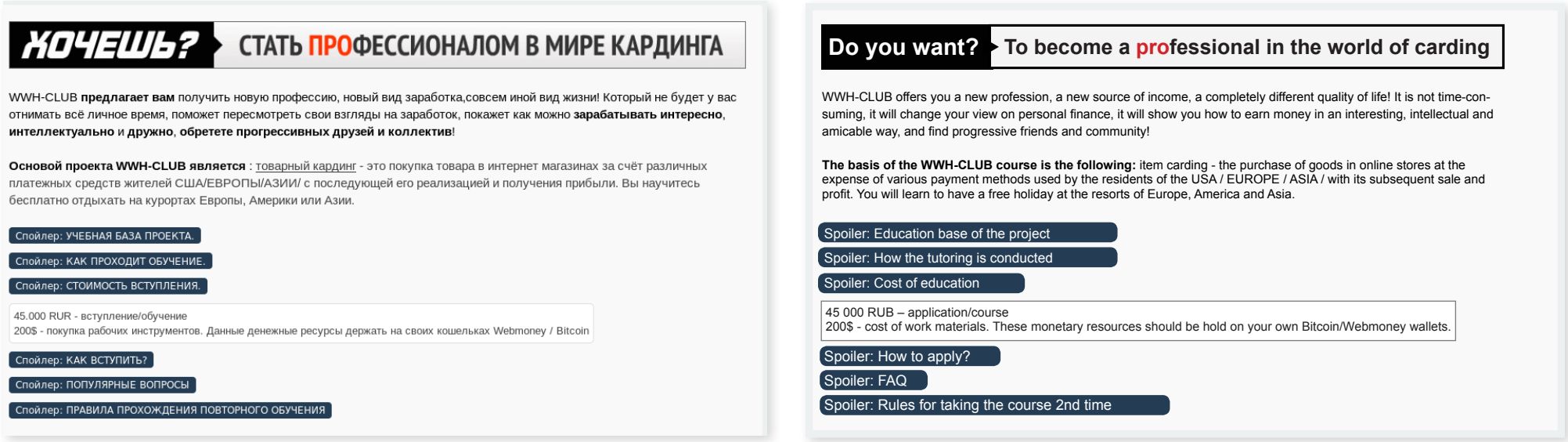


Figure 4: An advertisement for the WWH online course, with a translated version on the right hand side

The 6-week course is comprised of 20 lectures (see Figure 5), five expert instructors, webinars, detailed notes, course material (Figure 6), and question and answer sessions. The course instructors claim that, with this knowledge, carders can make more than $3,000 a month for 10-12 hours a week of work. Of course, fraudsters who work more than this can reap a higher profit, potentially making $12k a month, based on a standard 40-hour working week. For each lecture, which lasts between one and two hours, the number of attendees is capped at 15. The course is conducted in Russian, so it is specifically targeted at fraudsters in this geography. Given that the average monthly income in Russia is less than $700,[9] the appeal is understandable. To keep up to speed, retraining is offered every six months, although users would have to pay for the training over again.

Figure 5: The contents of the course

The course advertises itself across other forums, as seen in Figure 7, but relies on word of mouth in order to attract aspiring fraudsters. As one of their advertisements reads, (Figure 8), "We don't need PR." By charging almost $1000 for the 6-week course, this is a marked difference from the $1 guides available on dark web marketplaces.

Studying these guides and courses – especially the fresh and exclusive ones like WWH – can be useful to see what defenses the carders struggle to bypass, as well as the new tactics they have devised.

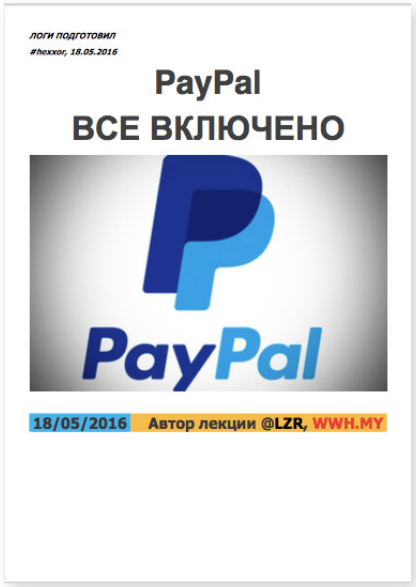


Figure 6: An example piece of course material provided, giving advice on how to bruteforce PayPal for carding purposes

Figure 7: An advertisement for the forum on a popular fake document site

Figure 8: A banner from the forum that reads "Biggest carding-forum -> wwh-club -> we don't need PR"

Stage 2: Buy payment cards from a reputable site

For those without the ability to harvest their own credit card details, there are plenty of options to buy. For the last two years, Alphabay – one of the largest market-places – introduced its own credit card shop. At the time of writing, Alphabay was down amid speculation of an exit scam. Whether or not AlphaBay resurfaces, there is no shortage of AVC shops online. In fact, a Google search for "CVV online shop" returns almost 25,000 results. Of course, many of these sites are scams and choos-ing between the shops can be difficult. The ability to auto-check (the act of testing the validity of a card by putting through a small charge) prior to purchase and the existence of escrow services are good indications of a reputable site. By searching for sites that offer an escrow service, our own analysis identified 70 English language carding domains and 151 Russian language carding domains. The total number of carding domains is likely to be higher, as our analysis focused on vBulletin forums.

To help cybercriminals make a selection, the online course suggests six carding sites. Examination of two of these sites offers insights into the number of accounts for sale across different card types (Figure 9) and geography (Figure 10). In just these two forums, more than 1.2 million payment cards were offered for sale. Visa was the most popular type of card with 783,008 cards and the United States and India were the most popular geographies, with 461,384 and 443,988 cards respectively. Of course, this is just a snapshot in time, based on the card details that are currently available; new data is added at least weekly. Overall, there is a bias towards the rich, western countries where card balances are likely to be higher. It is of little surprise that the Russian geography features little, given that the course explicitly forbids fraud against Russian cards. It is not uncommon to see Russian criminals specifically avoid targeting Russians so as not to strike the ire of law enforcement or intelligence agencies.

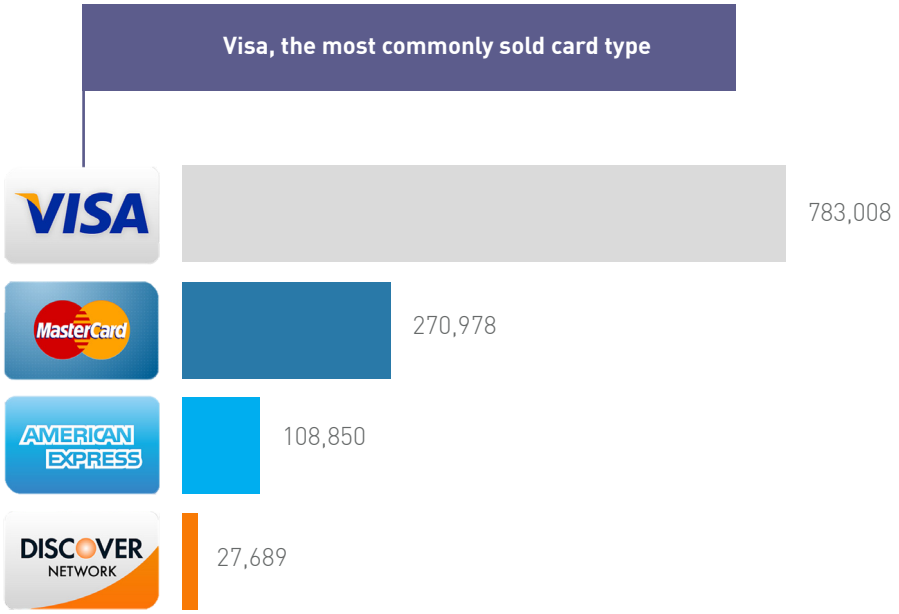


Figure 9: Credit cards for sale, distributed by card type

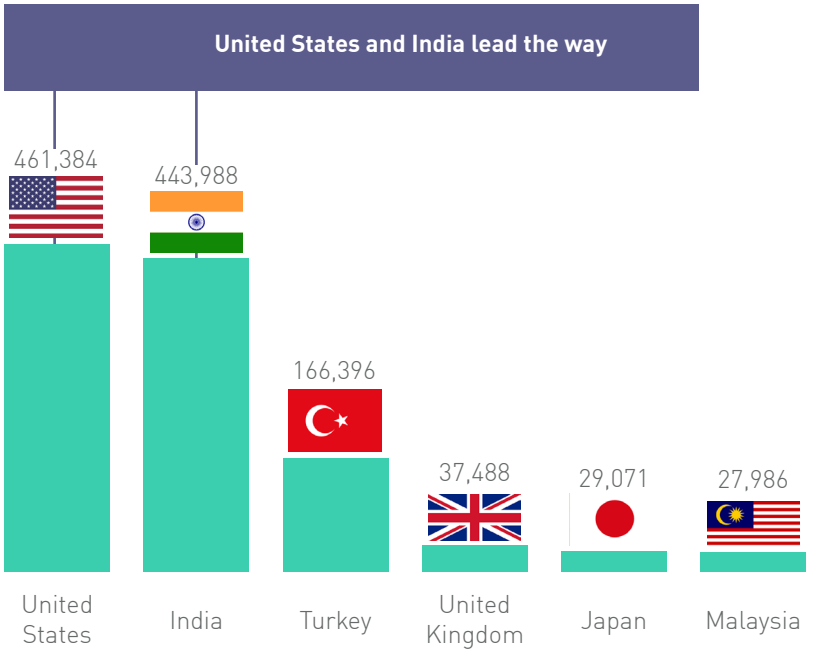


Figure 10: Credit cards for sale, distributed by geography

Even if an individual buys payment card information from a reputable vendor, there is no guarantee the card will still be in use or have a worthwhile balance. Not all data is of the highest quality, and different AVCs are likely to sell the same information. Most AVC shops worth their salt will provide a checking method (Figure 11) for customers to check the balance of a card before proceeding with the sale.

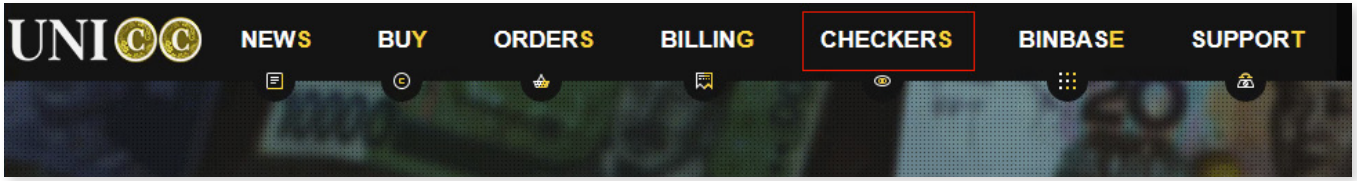


Figure 11: A screenshot of one recommended AVC, showing the "checkers" tab

For those purchasing cards on a site that lacks payment card validation, another method used to check the cards is an IRC room (Figure 12). For a nominal fee ($0.15), carders can use this method to check the balance of a particular payment card. This serves as a reminder that criminals do not need to cash out to make money from carding – there's plenty to be made from support services too.

The least expensive cards will be those requiring further authentication to cash out. The main obstacle to this is the PIN of the cardholder, which can be tricky and time-consuming to find out. Therefore, it is no surprise to see further services crop up such as the one shown in Figure 13, which is an automated service to call targets to socially engineer their PIN code. The service calls individuals and impersonates their bank, offering to set up additional security. In order to set up these security controls, the user inputs their PIN into their telephone. Successfully harvested PINs would then appear in the user's dashboard (Figure 13). The individuals promoting the service suggest targeting individuals in more rural locations. Although the legitimacy of this service cannot be verified, the shift towards social engineering as a service is an interesting development.[10]

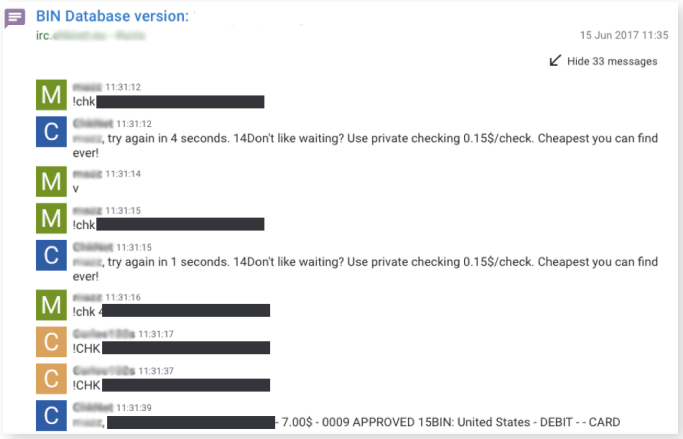


Figure 12: An IRC channel used to check balances of payment cards

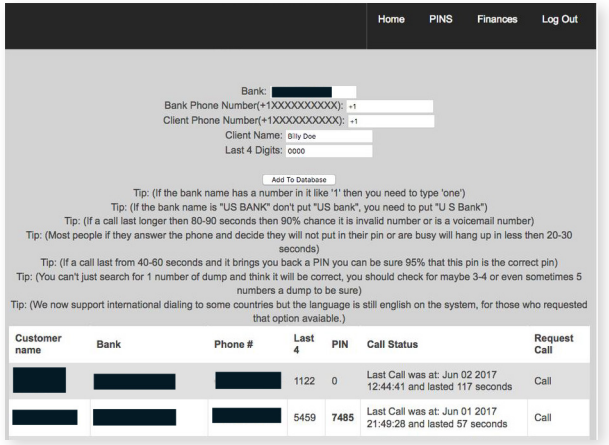


Figure 13: An online service for acquiring PINs from victims

Stage 3: Commit payment card fraud and cash out

As described above, there are many ways that cybercriminals make money in the carding ecosystem; different tiers will have different ways of generating revenue. The course recommends a range of techniques for cashing out. Here are three:

1. **Direct Purchase of Goods.** Fraudsters use sites that are cardable in order to make fraudulent purchases with stolen payment card information. A "cardable" site refers to a site susceptible to fraudulent purchases as a result of lax security controls (Figure 15). The sad reality is that not all ecommerce sites are compliant with the Payment Card Industry Data Security Suite. Worse yet, being PCI compliant doesn't mean you are secure. Criminals collaborate and share lists of cardable sites that individuals can turn to that allow goods to be purchased with stolen payment cards. The carder will then purchase goods and resell them for a reduced price in order to receive clean money (Figure 14). This will often entail reshipping scams, outlined on the following page.

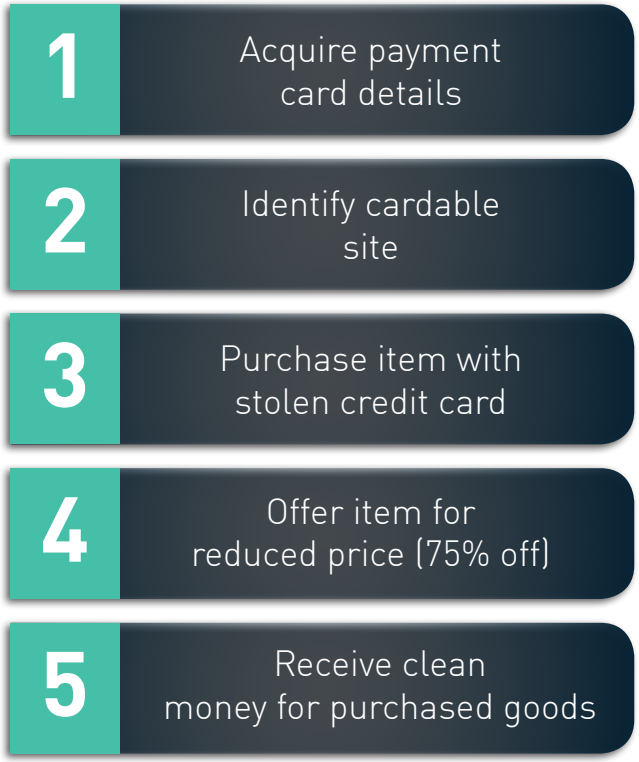


Figure 14: A fraudsters' process for purchasing goods


List of Cardable Sites - tested 01/17

Mostly for pleasure lol when the gf or the boys want something thought I'd share:

[redacted] bill=ship

[redacted] Sports - use non vbv cvv

[redacted] (got my entire [redacted] office a gift set) any cvv, any drop, no bill

[redacted], keep order under 300

[redacted] - car parts, they do phone verification super easy

[redacted] auto - keep order under 1000 and don't do FedEx expedited shipping

[redacted] - handcrafted dress shoes

[redacted] - they do phone verification very easy

[redacted] (expensive AF Persian rugs) - use non vbv cvv

[redacted] - order in store pickup, very easy tovpikcup under any name

[redacted] - cool stuff here, very easy to do

[redacted] - keep order under 400

[redacted] - keep order under 300

Figure 15: A list of cardable sites from 2017

2. Agent Fraud. Specific to hotels and airlines, one technique suggested is to impersonate an agent working with the target organization. The carder impersonates an agent, makes a reservation in the cardholder's name, waits for the card to authorize, and then changes the reservation name. Despite clear efforts made by law enforcement (153 criminals were detained in 64 countries last month for this type of fraud[11]) this seems to be a popular approach. Figure 16 is taken from another forum where carders discuss the success of this social engineering technique. As one user of the guide commented, "You just need some SE [social engineering] skills."

3. "Drops and Middlemen." This refers to a range of techniques, and the course provides detailed lectures on each. There are two main approaches to drops and middlemen:

a. Using legitimate companies that offer delivery methods for countries that do not offer international shipping (Figure 17). This is particularly useful for Russian fraudsters looking to purchase goods from U.S. sites.

b. Registering fake companies that search for unemployed and vulnerable people to take seemingly legitimate jobs as "Merchandising Manager" or similar. This job involves reshipping fraudulent goods and counterfeit money to safe addresses.[12] Just as with agent fraud, social engineering is key. The websites must look convincing in order to sway the individual to work for the bogus company. It is also a reminder to us that just because a website has https, does not mean it is a legitimate website. Criminals go out of their way to make the site look legitimate, which means individuals must be more vigilant.

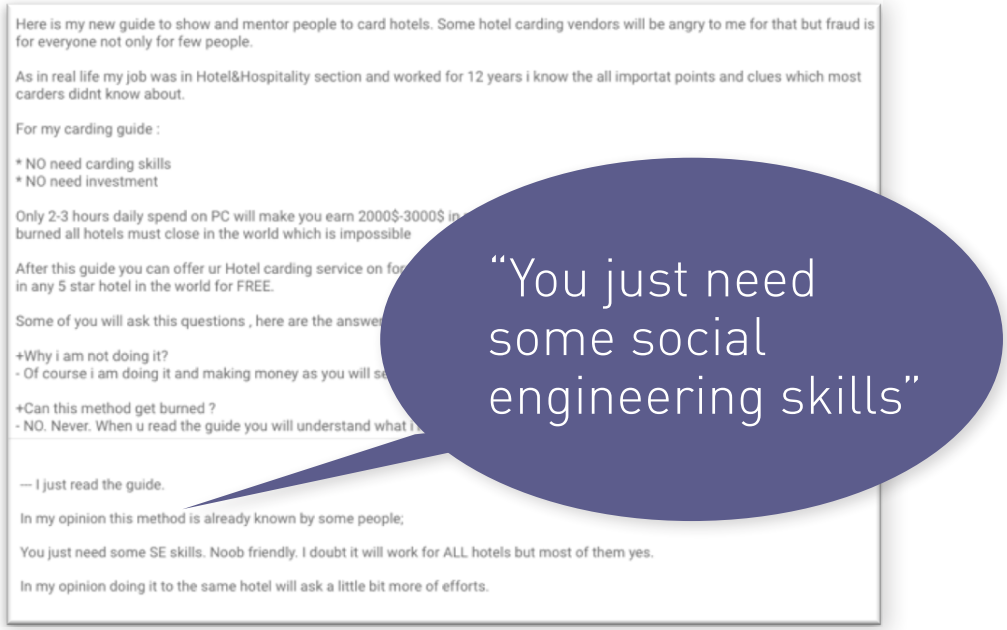


Figure 16: A dark web forum post discussing hotel fraud

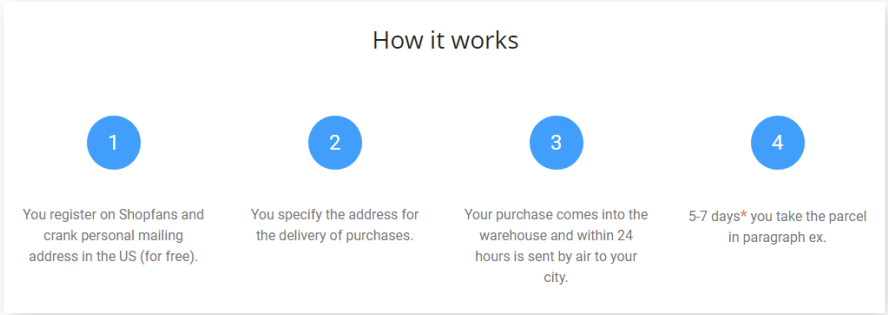


Figure 17: The website of a legitimate delivery service for Russians looking to purchase goods from U.S.-delivery only stores

Fraudsters score big

Payment card fraud is not new, nor are online guides and courses for the fraudsters. However, two developments mark a change. First, the increased professionalization of the training – including the instructors, lectures and training – demonstrates the potential profitability. Second, the carding industry is more specialized, with one reviewer describing the industry as "a society in which the participants form a niche, develop its own initiatives, build infrastructure...each of them in competition develops niche wants to be better [sic], coming up with new schemes."

Figure 18: Online course attendees post goods they have fraudulantly acquired online

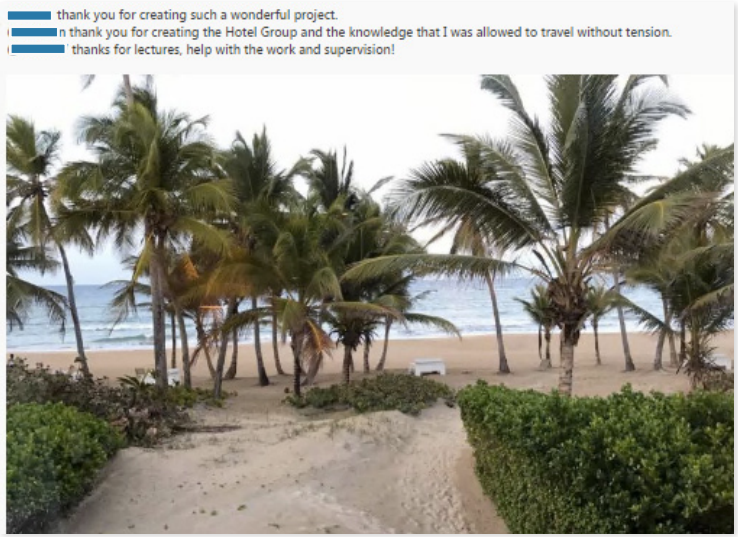


Figure 19: Photographs posted by a course attendee, thanking the course for their "Hotels" lecture

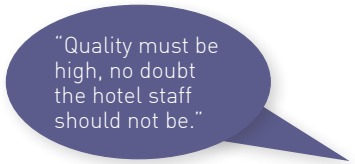
Judging by the positive reviews of satisfied students, there are real profits to be made. Figures 18 and 19 show a selection of images from fraudsters demonstrating their successes. While fraudsters may not stand to make as much potential money as harvesters and distributors, the right training enables entry level fraudsters to up their game to make far more money than they would otherwise earn. This has negative implications for credit card companies, merchants as well as consumers as increased fraud results in higher expenses and fees for all.

Within the carding industry, fraudsters will not necessarily remain fraudsters forever, given the chance to move up in the hierarchy. One user, for example, thanked the course as they were able to set up their own reshipping business. The increased sophistication and professionalization of the industry make payment card fraud a profitable opportunity for criminals and one with upward mobility.

A knowledge of carding trends helps defenders and consumers too

One review on the forum reads "do not worry: security and antifraud are not static but evolve and carding evolves with them." The reverse is true for defenders; carding is not static, but is also constantly evolving. The challenge for defenders is to keep up with the latest techniques and adapt to them. Combining knowledge of the carding ecosystem with specific tactics outlined in the course, it's clear that there are measures payment card companies, merchants and consumers can all take to create more friction for the fraudsters.

The quality of credit cards is certainly an important factor, but what is striking about many of the courses' techniques are the emphasis on social engineering. The course offers an entire week's lecture titled "Warming up the shop." This lecture provides advice on how to socially engineer people through knowledge of their local area in order to build rapport with the target. As the instructor puts it, "That's why I always advise to watch the news. Because with such incidents, it is possible to play beautifully." As another instructor aptly put it, "Quality must be high, no doubt the hotel staff should not be." Carders are not (all) blindly putting in card numbers into retail sites hoping to make a purchase; they are being trained to learn their target's surroundings and processes. Defenders can similarly study the carders; understand what techniques they use, the organizations they target and the cards they target. In doing so, organizations can increase the friction at every stage of the carders' process.



Payment Card Companies	Merchants	Consumers
Detect phishing with DNS Twist. Proactively monitor for permutations on your domain name, which could help you to detect any criminal seeking to harvest information from your customers.	**Learn about latest techniques.** Criminals will do what they can to avoid friction. If certain banks have better anti-fraud measures, the instructors recommend avoiding them. Understand what makes carding difficult. For example, 3D Secure is an additional layer of security deployed by Visa and Mastercard and proven to be a real obstacle for criminals.	**Be picky about who you shop with.** If shopping somewhere new, ensure the shop uses 3D Secure. This is a proven deterrant to fraudsters.
Understand threats against your customers. Monitor the activity of banking trojans, such as Trickbot, to identify patterns in their targeting and techniques used to gain access to your customers' computers.	**Make security as important as user experience.** There must always be a balance between security and user experience, but online merchants should be aware that criminals are turning to mobile apps to commit payment card fraud as it provides them with less obstacles.	**Take care when booking travel and hotels.** Offers that appear too good to be true often are. Act with caution if using a travel agent you have not previously used; this is a common scam for fraudsters.
Monitor AVC shops for BINs and IINs. Monitor for Bank Identification Numbers (BINs) and Issuer Identification Numbers (IINs) that are offered for sale. In many cases, it is possible to free text search and filter by BIN numbers.	**Monitor for mentions of cardable sites.** Criminals share lists of cardable sites; if your company name crops up, it's a good indication that you are experiencing fraud. Companies can search with the help of Google Alerts or open source web crawlers like Scrapy to look for mentions of their brands.	**Don't be part of a cashing-out scam.** Be wary of job postings offering well-paid jobs to re-ship goods, often offering to work from home. Fraudsters go to great lengths to make these companies look legitimate.
Monitor IRC checking channels. Monitor IRC checking channels for BINs and IINs that are indicative of a criminal testing an individual's card.	**Train your staff and your customers.** Remember that the most advanced methods all involved social engineering. Europol provides great advice for consumers.[13]	**Protect your PIN.** Fraudsters are constantly developing new and innovative ways to extract your sensitive data. Never share your PIN over email or phone, even if they claim to be from your bank.
Benchmark yourself against peers. Understand which card providers fraudsters recommend **not** using, and use this to understand where your company stacks up.	**Don't be part of the problem.** Cashing out is only one small part of the fraud; the harvesting of credit card information is required first. Protect your customers' credit card information by storing the information securely and ensuring payment software is patched.	**Check statements carefully.** Check your bank statements carefully for irregular purchases – even those that appear in a nearby location. Alert your bank if you suspect fraudulent activity.

Glossary

AVC – Automated Vending Carts are shops that specialize in the sale of credit card information.
Bank Drop - A bank account opened with fraudulent credentials.
BIN – Bank Identification Number
Cashing Out – The process of turning fraudulent transactions into money.
CNP Fraud – Card Not Present Fraud, where no physical copy of a card is made and all the fraud is committed online.
Cloning – Physical creation of new cards that take the characteristics of those that have been skimmed.
CVV – Card Verification Value
EMV – A credit card standard created by Europay, MasterCard and Visa, now synonymous with "Chip and Pin."
IIN – Issuer Identification Number
IRC – Internet Relay Chat
PCI-DSS - The Payment Card Industry Data Security Standard (PCI-DSS) is a proprietary information security standard for organizations that handle branded credit cards.
Skimmer – Device used to capture credit card information.

End Notes

1. 'Point-of-Sale Card Fraud Predicted to Decrease as Card Not Present and New Account Fraud Increases,' https://www.javelinstrategy.com/press-release/point-sale-card-fraud-predicted-decrease-card-not-present-and-new-account-fraud
2. 'Online Fraud Expected To Grow 43 Percent This Holiday Season In The US,' http://www.pymnts.com/news/security-and-risk/2016/us-online-fraud-43-percent-growth-holidays-cybersecurity/
3. 'Annual online card spending will double to $6 trillion by 2021,' https://cardnotpresent.com/annual-online-card-spending-will-double-to-6-trillion-by-2021-report/
4. 'Credit card fraud in130 000 cases organised crime group disrupted n european cross border action,' https://www.europol.europa.eu/newsroom/news/credit-card-fraud-in-130-000-cases-organised-crime-group-disrupted-in-european-cross-border-action
5. 'Point-of-Sale Card Fraud Predicted to Decrease as Card Not Present and New Account Fraud Increases,' https://www.javelinstrategy.com/press-release/point-sale-card-fraud-predicted-decrease-card-not-present-and-new-account-fraud
6. 'Russian born cybercriminal sentenced over nine years prison, https://www.justice.gov/usao-edva/pr/russian-born-cybercriminal-sentenced-over-nine-years-prison
7. 'Russian Hacker Sentenced to 27 Years in Credit Card Case,' https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html
8. 'Reshipping Scam,' https://postalinspectors.uspis.gov/radDocs/consumer/ReshippingScam.html
9. 'Russia Average Monthly Wages,' https://tradingeconomics.com/russia/wages
10. 'This Dark Web Site Creates Robocalls to Steal People's Credit Card PINs,' https://motherboard.vice.com/en_us/article/3knz98/dark-web-site-robocalls-to-steal-credit-card-pins
11. '153 detained for ticket fraud following worldwide law enforcement operation,' https://www.europol.europa.eu/newsroom/news/153-detained-for-ticket-fraud-following-worldwide-law-enforcement-operation
12. 'Reshipping Scam,' https://postalinspectors.uspis.gov/radDocs/consumer/ReshippingScam.html
13. 'E-commerce tips and advice to avoid becoming fraud victim,' https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/e-commerce-tips-and-advice-to-avoid-becoming-fraud-victim

About Digital Shadows

Digital Shadows monitors and manages an organization's digital risk across the widest range of data sources within the visible, deep, and dark web to protect an organization's business, brand, and reputation. The Digital Shadows SearchLight™ service combines scalable data analytics with human data analysts to manage and mitigate risks of an organization's brand exposure, VIP exposure, cyber threat, data loss, infrastructure exposure, physical threat, and third party risk, and create an up-to-the minute view of an organization's digital risk with tailored threat intelligence. The company is jointly headquartered in London and San Francisco.
For more information, visit www.digitalshadows.com.

U.S. Headquarters
Digital Shadows, Inc.
332 Pine Street, Suite 600
San Francisco, CA 94104

North American Intelligence Operations Hub
5307 E. Mockingbird Ln.
Suite 915
Dallas, TX 75206

UK Headquarters
Digital Shadows, Ltd.
Level 39
One Canada Square
London E14 5AB

digital shadows_