



SecureWorks

# Underground Hacker Markets

ANNUAL REPORT—APRIL 2016







# Price List for Hacker Goods and Services

## Credit Cards

	Price in 2013	Price in 2014	Recent Prices
Visa and MasterCard (U.S.)	\$4	\$4	\$7
Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data	\$12	\$12	\$15
Visa Classic and MasterCard (Canada, Australia, and New Zealand) with Track 1 and Track 2 Data	\$19 – \$20	\$19 – \$20	\$25
Visa Classic and MasterCard Standard (EU) with Track 1 and 2 Data	\$28	\$28	\$40
Visa Classic and MasterCard Standard (U.K) with Track 1 and Track 2 Data	\$19 – \$20	\$19 – \$20	\$40
Visa Classic and MasterCard Standard (Japan and Asia) with Track 1 and Track 2 Data	\$28	\$28	\$50
Premium Visa and MasterCard (U.S.) with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$30
Premium Visa and MasterCard (EU and U.K.) with Track 1 and 2 Data		\$23 (V); \$35 (MC)	\$50 – \$60
Premium Visa and MasterCard (Canada, Australia and New Zealand) with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$35 for V and MC
Premium Visa and MasterCard (Japan and Asia) with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$80 for V and MC
Premium American Express Card (U.S.) with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$30
Premium Discover Card (U.S.) with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$30
VBV (U.K., Australia, Canada, EU and Asia)	\$17 – \$25	\$28	\$25

## Hacking Email and Social Media Accounts

	Recent Prices
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	\$129
Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)	\$65 – \$103
Popular Ukranian Email Accounts (Ukr.net)	\$129
Popular U.S. Social Media Accounts	\$129
Popular Russian Social Media Accounts (VK.ru and Ok.ru)	\$194
Corporate Email Accounts	\$500 per mailbox
IP address of Computer User	\$90

## Tools

	Price in 2013	Price in 2014	Recent Prices
Remote Access Trojans (RATs)	\$50 – \$250	\$20 – \$50	\$5 – \$10
Crypters	N/A	\$50 – \$150	\$80 – \$440
Angler Exploit Kit			\$100 – \$135

## Identities, Passports, Social Security Cards and Other Documents

	Price in 2013	Price in 2014	Recent Prices
US Fullz	\$25	\$30	\$15 – \$65
Fullz (Canada, U.K.)	\$30 – \$40	\$35 – \$45	\$20 (Canada) \$25 (U.K.)
U.K. Passport Scan			\$25
Physical Counterfeit Passports (non-U.S.)	N/A	\$200 – \$500	\$1,200 to \$3,000 (European)
Physical Counterfeit Passports (U.S.)			\$3,000 to \$10,000
Templates for U.S. Passports			\$100 – \$300
New Identity Package, including scans of Social Security Card, Driver's License and, matching utility bill		\$250; matching utility bill an additional \$100	\$90
Physical Counterfeit Social Security Cards		\$250 – \$400	\$140 – \$250
Scans of Counterfeit Driver's License			DL Scans \$14 – \$20 (U.S.) \$14 (U.K., CANADA)
Physical Counterfeit Driver's License (France)			\$238
Physical Counterfeit Driver's License (U.S., U.K., Germany, Israel, International Driver's Permit)		\$100 – \$150	\$173

## Online Accounts

	Recent Prices Price based on account balance
Popular U.S. Online "Business" Payment Account Credentials	Ranges from \$20 – 149
Transfer Funds from Popular Online Payment Account to Buyer's Account of Choice	\$750 cost \$226 \$1,500 cost \$377 \$1,520 cost \$385 \$2,290 cost \$573 \$2,999 cost \$750 \$3,799 cost \$950
Popular U.S. Online Payment Account Credentials	\$330 cost \$80 \$400 cost \$160 \$500 cost \$240 \$600 cost \$320 \$950 cost \$600

## Bank Accounts; Airline and Hotel Points

	Recent Prices
Bank Account Credentials	Price based on account balance
Bank accounts – ANZ (Australia)	\$18,000 cost \$4,750
Bank accounts – ANZ (Australia)	\$22,000 cost \$2,250
Bank accounts – ANZ (Australia)	\$62,567 cost \$3,800
Bank accounts with no balance listed – Turkey, Sweden, Norway, Romania, Bulgaria, Croatia,	\$400 (flat fee)
Bank accounts – (U.K.)	\$27,003 cost \$2,000
Bank account – (U.S.)	\$1,000 cost \$40
Bank account – (U.S.)	\$2,000 cost \$80
Bank account – (U.S.)	\$4,000 cost \$150
Bank account – (U.S.)	\$7,000 cost \$300
Bank account – (U.S.)	\$15,000 cost \$500
High Quality Bank Accounts with Verified, Large Balances of \$70,000 – \$150,000	6% of the balance of the account
Large U.S. Airline Points Accounts – varies based on amount	Price based on points in account 1,500,000 points cost \$450 300,000 cost \$90 200,000 cost \$60
Large Middle East Airline Points Accounts – varies based on amount	Price based on points in account 500,000 cost \$150 450,000 cost \$90 250,000 cost \$50
Large International Hotel Chain Points Account	Price based on points in account 1,000,000 points cost \$200 400,000 cost \$80 300,000 cost \$60 200,000 cost \$40 100,000 cost \$20 50,000 cost \$10

## Hacking Services

	Price in 2013	Price in 2014	Recent Prices
Hacking Tutorials	N/A	\$1 each to \$30 for 10 (depending on the tutorial)	\$20 to \$40 for multiple tutorials
Hacking Website (stealing data)	\$100 – \$300	\$100 – \$200	\$350
DDoS Attacks	Per Hour: \$3 – \$5 Per Day: \$90 – \$100 Per Week: \$400 – \$600	Per Hour: \$3 – \$5 Per Day: \$60 – \$90 Per Week: \$350 – \$600	Per hour: \$5 – \$10 Per Day: \$30-\$55 Per Week: \$200 – \$555
Doxing	\$25-\$100	\$25-\$100	\$19.99



service they are purchasing will be satisfactory. In fact, one seller of email hacking services states in their ad: "Work through the Guarantor Service is welcome," and "no-prepayments, you pay only for visible results—we will present the necessary proof." The hackers' willingness to work through a "guarantor" seemed to indicate that the sellers on the Russian Underground aim to please and will do what it takes to ensure they continue to deliver the very "Best Customer Service."

Our security experts also saw lots of hacker/sellers advertising their outstanding attributes. One seller who was offering customers the service of "hacking into organizations" states in their ad:

"Why choose us?"

- Professionalism. We are working only with the best technologies and developments
- Experience. We are constantly improving our technology in this area and are adopting new advanced solutions
- Quality. Our expertise allows us to exploit various vulnerabilities on the target servers, making our attacks the most effective.
- Power. With the continuous improvement of our technology, we have huge abilities
- Anonymity. You can be sure that any information regarding your order will not be shared with a third party.
- Honesty. We provide conditions for repayment of funds, if you are not entirely satisfied.
- Provide free-trial attacks on web servers.
- We are Trustworthy and Professional."

Our security experts also saw several hacker/sellers advertising their outstanding attributes.



The hacker goes on to state that, “Buyers have, at their disposal, access to all of the following items after he/she has hacked the email account of the victim”:

- Access to all the websites registered by the owner of the email account
- Personal correspondence and confidential data of the victim
- Exact details regarding the date/time of the email account hack
- Ability to make changes to the victim’s mailbox—including changing the username and password, ability to change the design of the email account and even remove the email account permanently

Rates the hacker charges for hacking an email or social media account are listed in Table 1. The seller accepts payment via WebMoney and Yandex.Money.

### DDoS Attacks; Free 5-10 Minute DDoS Tests Offered

Providing DDoS Attacks remains a popular service offered by hackers on the underground hacker markets, including the Russian markets. One of the hackers selling their DDoS skills states in a forum that he is happy to “offer their services so as to address the websites and forums of your competitors using DDoS Attacks, and that they will take on virtually any projects ranging from servers, which have weak protection to servers with high protection!” They go on to state that “their service is a quick solution to your problems with competitors and enemies.”

Still another hacker selling DDoS services offers “an attack on any computer port that you specify with complete anonymity.” The hacker also promises that “long time, regular customers and wholesale customers

receive big discounts,” and that he is online 24X7. He offers the “best value for the money,” and if you have any problems, “a money back guarantee.” He then goes on to state that the “services does not violate the law,” which our security experts found quite amusing.

The security experts did find that most of the Russian hackers they observed who were offering DDoS Attack services were willing to perform a free 5- to 10-minute DDoS test for customers.

They discovered that DDoS Attack services on several of the Russian Underground markets cost the following:

- \$5 per hour
- \$50 per day
- \$200 to \$350 per week (the higher price is charged if the target website has anti-DDoS protection installed)
- \$1,000 per month

Plus, most of the hackers offer a variety of DDoS attacks including:

- UDP Flood
- TCP Flood
- HTTP/HTTPS Flood
- SYN Flood

The hackers accept WebMoney and Yandex.Money, and some accept Bitcoin.

**Table 1: Rates for hacking social media and email accounts**

<b>Mail.ru</b>	5,000 rubles (approximately \$65)
<b>Yandex.ru</b>	7,000 rubles (approximately \$90)
<b>Rambler. Ru</b>	8,000 rubles (approximately \$103)
<b>Ukr.net</b>	10,000 rubles (approximately \$129)
<b>Gmail.com, Yahoo.com, Hotmail.com</b>	10,000 rubles (approximately \$129)
<b>Facebook.com</b>	10,000 rubles (approximately \$129). Please note: the victim’s password stays the same.
<b>IP address of computer user</b>	7,000 rubles (approximately \$90)
<b>Corporate email account</b>	\$500 per mailbox
<b>Vkontakte (VK) social media account</b>	15,000 rubles (approximately \$194)
<b>Odnoklassniki (OK.ru) social media account</b>	15,000 rubles (approximately \$194)



# Hacker Goods for Sale

Bank Accounts, Popular Online Payment Accounts, Airline Points Accounts, Credit Cards, Hacker Tutorials...You Name It



The smaller the balance in the account, the higher the seller's fee. For example, one U.S.-based account with a balance of \$1,000 was selling for \$40, while another U.S.-based account with a \$50,000 balance was selling for \$587.

## Internet Bank Account Credentials

Just as there is no lack of credit cards for sale on the underground markets, there is no lack of bank account credentials for sale. Our security experts saw stolen bank credentials for accounts located in the U.S, U.K., Denmark, Sweden, Croatia, Turkey and Australia. The hackers were selling the credentials for anywhere from 1 percent up to 5 percent of the account balance. The smaller the balance in the account, the higher the seller's fee. For example, one U.S.-based account with a balance of \$1,000 was selling for \$40, while another U.S.-based account with a \$50,000 balance was selling for \$587. However, our

security experts did come across credentials for accounts based in the U.K. and Europe that were selling for a flat \$400. In that case, the seller did not list the balance in the account publicly. One wonders if bank account credentials, like credit cards in the U.K. and Europe, are more expensive because they are harder to come by due to there being fewer breaches involving this type of data.

## Online Payment Accounts Sell for a Hefty Fee

Just as one's bank account credentials reap hefty prices on the underground, so do account credentials for popular online payment accounts because in many ways they are very similar to a bank

account. However, many online payment accounts do not have the same level of fraud alerts that larger banks employ. We found hackers selling the credentials for “personal” and “business” online payment accounts. In fact, these credentials, depending on the balance in the account, often sell for more than bank account credentials, in regards to the percentage of the balance charged. Cashing out these types of accounts, especially if the account owners do not implement the two-factor authentication option, can be very simple for the criminal. Our security experts found numerous Hacker Tutorials outlining how one can easily cash out these accounts, especially when there is actual cash sitting in the accounts. Our security experts found hackers willing to transfer the balances of online payment accounts to the account of your choice, whether it be a bank account, an online payment account, and so on. This is not cheap of course, since they are taking the risk. For example, one hacker was willing to transfer \$750 for \$226, while the same hacker was charging \$377 to transfer \$1,500 from an online payment account.

### **Need a Cheap Vacation Anyone? Airline and Hotel Points Accounts on the Auction Block.**

If you think you are the only one interested in your frequent flyer points and hotel points, think again. As we have previously pointed out, hackers have a way of monetizing almost any piece of data, and this includes your frequent flyer accounts and your hotel points accounts. Our security experts found hackers on English-speaking sites selling frequent flyer account credentials for a variety of large U.S.- and Middle

East-based airlines. The prices were for the following: an account with 1,500,000 points cost \$450, while another frequent flyer account with 300,000 points cost \$90. The hackers were also selling credentials for hotel accounts, associated with many of top hotel chains.

For example, a brand-name hotel account with 100,000 points sells for \$20, and an account with 50,000 points runs \$10. Clearly, the airline points accounts are deemed more valuable by the sellers than the hotel points, though \$10 here and \$20 there can add up.

One is probably asking why would a scammer want to purchase someone’s frequent flyer or hotel points account number? Well, the answer is simple. There are legitimate websites where one can trade their airline and hotel points for gift cards. For example, on the site <https://www.points.com/#/>, 6,412 reward points for a major U.S. airline could be exchanged for a \$25 gift card to a number of popular chain restaurants, while 12,294 points was enough for a \$50 gift card to a high-end retail store.

Scammers also have the potential of cashing out airline points for cash via online businesses called mileage brokers. Although that activity is deemed a no-no with the airlines, scammers are clearly not worried about breaking any of their rules since they are purchasing stolen points in the first place. One such site offering cash for points is called <http://flipmymiles.com/>. On their FAQ, they state:

#### **Q: How much will I get paid?**

This depends on the type of points or miles sold but we pay at the most competitive

industry rates ranging upwards of a penny to the point. To give you an idea, we pay anywhere from \$1,000 to \$1,500 for a 100,000 points. Compared to the \$500 to \$1,000 your credit card company would pay you, that’s quite the difference.

### **Credit Cards for Sale**

As in prior years, the market for stolen credit and debit cards is bustling and knows no geographic bounds. Throughout the dark web, interested buyers can find credit card information from countries all over the world, from the U.S. to Japan to Australia. And while the damage a stolen credit card can potentially do is significant, the cards themselves are relatively cheap – a stolen U.S. MasterCard or Visa card (without Track 1 or Track 2 data) could be purchased for just \$7, a slight increase from 2014 and 2013 when those cards sold for \$4.

Not surprisingly, cards with Track 1 and Track 2 data were more expensive, and in some cases rose significantly in price compared to previous years. For example, while our security experts found prices for such cards from the U.S. selling for as little as \$12 in 2014, recently, cybercriminals were spotted selling U.S. Master Card and Visa cards with Track 1 and Track 2 data for \$15. While cards with Track 1 and Track 2 data from the UK sold for \$19–\$20 in 2014, Dell SecureWorks has observed Master Card and Visa cards from the UK with that data selling for \$40. In Japan meanwhile, Visa and Master Cards with Track 1 and Track 2 data sold for \$50.

Premium cards from each of the major brands were the most expensive, reaching \$30 for

MasterCard and Visa cards from the U.S. with Track 1 and Track 2 data. Those same cards from the U.K. sold for as much as \$60, while in Japan the price was \$80.

As an additional boost to fraudsters, underground marketplaces make VBV (Verified by Visa) data available as well. A security measure meant to protect cardholders, VBV is another password or piece of data assigned to Visa cardholders to defend against fraud. VBV data for cardholders in the U.K., Asia, Canada and Australia dipped slightly in value compared to 2014, dropping from \$28 to \$25.

### Stolen Identities, Passports, Social Security Cards and Other Documents

Identity theft is the stock and trade of many criminal hacker groups, and for good reason. A scammer who can impersonate an unsuspecting victim can open the door to all kinds of crimes, such as bank fraud and insurance fraud. For that reason, documents that can be used to impersonate another individual, especially those with impeccable credit, are worth their weight in gold. Often, this type of information is sold in packages. The prices for these packages — as well as the items

individually — vary from market to market. In one instance, our security experts discovered a package that included a social security number, driver’s license and a matching utility bill being offered for \$90.

Relatively cheap packages of data known as Fullz are also bought and sold on the criminal underground. Fullz — what hackers call a dossier of credentials for an individual that can be used to commit fraud — typically include data such as names, addresses, and social security numbers in combination with one or more of the following: bank account information, online banking credentials, or credit card numbers. Recently, our security experts saw Fullz selling for \$15 for a U.S. victim.

There was a difference in pricing between when cybercriminals offered physical counterfeit social security cards or scans of cards, versus when they offered just the social security numbers. The cost of physical counterfeit social security cards spotted by Dell SecureWorks ranged from \$140 to \$250, a significant drop off from 2014, when those items were sold for between \$250 and \$400 each. A physical counterfeit Canadian Social

Identification Number card — which is similar to a social security number in the U.S. — was observed being sold by cybercriminals out of China for approximately \$173.

The price of driver’s licenses varied, too. A physical counterfeit French driver’s license was spotted being sold by one vendor for approximately \$238, while German, U.S., Israeli, U.K. and international driver’s permit sold for about \$173.

Currently, the price for an actual U.S. passport ranges from \$3,000 to as high as \$10,000. The higher the quality, the higher price. Templates for U.S. passports sold anywhere from \$100 to \$300, and the buyer must find their own printer. Passports for European countries have been seen going for between \$1,200 to \$3,000. Beyond financial scams, the trafficking of these kinds of items can have other potential implications as well. For example, [an ABC report](#) in December 2015 noted that authorities in the U.S. suspected that the terrorist group ISIS had the ability to print legitimate-looking Syrian passports so that their members could travel undetected.

These are not the only documents worth their weight in gold to criminals trafficking in stolen identities. Utility bills are also offered in many deals as part of the package — for the price of the \$90 mentioned above for example, one seller offered a scan of a social security card, a driver’s license (for California, Nevada, Connecticut, or Florida) and a matching utility bill. According to our experts, the price for such packages depends on the number of documents involved, and in some cases could go up if the seller is providing additional help creating

**Table 2: Rates for premium credit cards with Track 1 and Track 2 data**

Credit Card	Recent Prices*
American Express (U.S.)	\$30
Discover Card (U.S.)	\$30
MasterCard and Visa (Australia)	\$35
MasterCard and Visa (U.K.)	\$50 to \$60
MasterCard and Visa (Japan)	\$80

\*All prices are in USD

the identity and guiding the buyer through the process.

### Shopping Mall for Malware

Malware is still an effective weapon in the holster of hackers targeting end-users. Remote access Trojans (RATs) are malware programs that have a backdoor that hackers use to gain administrative control of a compromised machine. Some of the cheaper and more accessible RATs on the forums our security experts examined included: BlackShades, AlienSpy, and DroidJack. Some RATs were spotted being sold for between \$5 to \$10, compared to \$20 to \$50 in 2014. Typically, the longer a RAT has been accessible on the underground, the cheaper it is. Hackers often look for free or cheap RATs to run through programs called crypters that encrypt the malware and make it more difficult for security programs to detect. Crypters were sold for prices ranging from \$80 to \$440. Among the most popular ones were Aegis, Inferno Worm, Beef and Spoof and Pandora rat. It is not clear

what caused the spike in the Crypter prices that our security experts saw.

Exploit kits are also a common item on the digital shelves of the underground market. Exploit kits seek to identify and exploit software vulnerabilities on targeted computers. They are typically designed to be modular and are often updated to add newer exploits to replace older ones. One of the most popular exploit kits continues to be Angler, which first appeared in 2013, and in 2015 was linked to the use of several zero-day vulnerabilities in the Adobe Flash Player. The Angler exploit kit was observed selling for between \$100 and \$135.

### How-to for Hackers

Hackers are not just interested in selling malware and stolen information. They also sell tutorials to help other budding criminals launch their own operations. In 2014, the cost for the tutorials ran from \$1 each to \$30 for 10, depending on the tutorial. Recently, buyers could

expect to purchase multiple tutorials for between \$20 and \$40. The tutorials cover a number of subjects, such as Denial of Service (DoS) Attacks, cracking Wi-Fi, Crypters and phishing. In some cases, these tutorials explain for example what a Crypter, a RAT and an exploit kit is, how are they used and how much hackers should pay for these hacker tools. Taken in combination with the easy-to-use tools, the tutorials certainly help to lower the barrier to entry for new hackers wanting to break into cybercrime.

The price for an actual U.S. passport ranges from \$3,000 to as high as \$10,000. Templates for U.S. passports sell anywhere from \$100 to \$300, and the buyer must find their own printer.













Mandate the use of two-factor authentication for all remote access solutions and for all company employees and business partners

- Remove Local Administrator rights for users. Attackers often take advantage of users that have of elevated privileges
- Back up all data (not just critical data), and document and rehearse contingency plans
- Audit privilege domain account usage, including administrator and service accounts
- Segment sensitive data on the network and closely monitor choke points

### Build Strong Technology Defenses

- Install firewalls around your network and web applications
- Deploy Intrusion Prevention Systems or Intrusion Detection Systems ([IPS/IDS](#)), which inspect inbound and outbound traffic for cyber threats and detect and/or block those threats
- Host Intrusion Prevention Systems (IPS)
- Use [Advanced Malware Protection](#) solutions for the [endpoint](#) and network
- Employ [vulnerability scanning](#)
- Institute 24x7 log monitoring, and web application and network scanning
- Take advantage of [security intelligence](#) around the latest threats (people working on the latest threats in real time, human intelligence)
- Use encrypted email

We also advise organizations with valuable data to implement an endpoint security solution across their environment which is focused on threat actor behavior and determining if an activity within one's network is malicious or not. The solution should be able to:

- Assess the host for known and unknown threats
- Monitor for threats attempting to maintain persistence
- Monitor process creations and associated files
- Examine thread injection events looking for adversaries moving between processes
- Examine network connection data at the host level to identify suspicious communications being sent to and from the host
- Monitor DNS activity at the host level

# Steps for Individuals

## For Safe Banking and Online Bill Pay

- Use a computer dedicated only to doing online banking and bill pay. That computer or virtualized desktop should not be used to send and receive emails or surf the web, since web exploits and malicious email are two of the key malware infection vectors.
- Be extra cautious when withdrawing money from an ATM:
  - Cover the keypad with your other hand when entering a PIN
  - Try to avoid nonbank locations where the ATM is in a hidden location that thieves could easily access without being detected
  - Check your bank and credit card statements regularly for fraudulent activity
- Consider subscribing to a 3 in 1 credit monitoring service to alert you when new credit or bank accounts are applied for, credit balances go over the norm, etc.

## Using Your Computer Safely

- Avoid clicking on links or attachments within emails from untrusted sources. Even if you recognize the sender, you should confirm that the sender sent that email, before clicking on any links or attachments.
- Make sure your anti-virus software is current and can protect against the latest exploits. Also, make sure that your anti-virus vendor has signatures for detecting the latest Trojans and that you have the most up-to-date anti-virus protections installed.
- Do not use “trial versions” of anti-virus products as your source of protection. Trial versions of anti-virus products are good for testing products, but do not continue to use the trial version as your protection for your home or work PC. The danger is that the trial version does not receive any updates, so any new Trojan or virus that is introduced after the trial version was released will have total access to your PC.
- Make sure you have your security protections in place. Software patch management is key. It is critical that you install updates for your applications and for your computer’s operating system as soon as they become available.
- Be cautious about installing software (especially software that is too good to be true — e.g., download accelerators, spyware removal tools), and be conscientious about pop-ups from websites asking users to download/execute/or run otherwise privileged operations. Often this free software and these pop-ups have malware embedded.



It is critical that you install updates for your applications and for your computer’s operating system as soon as they become available.



# Glossary of Terms

**Credit Card Track 1 and 2 Data** — Track 1 and 2 data is information that is contained in digital format on the magnetic stripe embedded in the back of the credit card. Some payment cards store data in chips embedded on the front side. The magnetic stripe or chip holds information such as the primary account number, expiration date, card holder name, plus other sensitive data for authentication and authorization.

**Distributed Denial of Service (DDoS) Attacks** — DDoS Attacks are the act of throwing so much traffic at a website, it takes it offline.

**Fullz** — Fullz is a dossier of credentials for an individual, including Personally Identifiable Information (PII), that can be used to commit identity theft and fraud. Fullz usually include: full name, address, phone numbers, email addresses (with passwords), date of birth, social security number (SSN) or Employee ID Number (EIN), and one or more of the following: bank account information (account and routing numbers, account type), online banking credentials (varying degrees of completeness), or credit card information (including full Track 2 data and any associated PINs).

**Odnoklassniki** — This is a social network service for classmates and old friends. It is popular in [Russia](#) and former Soviet Union.

**Personally Identifiable Information (PII)** — This is information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context. Some examples of PII are a person's full name, address, birthdate, driver's license number, telephone number and email address.

**QIWI** — This is a publicly traded [Russian payment service provider](#) headquartered in [Nicosia \(Cyprus\)](#), that operates electronic online payment systems primarily in Russia, Kazakhstan, Moldova, Belarus, Romania, the U.S and the United Arab Emirates.

**VBV (Verified by Visa)** — VBV works to confirm an online shopper's identity in real time by requiring an additional password or other data to help ensure that no one but the cardholder can use their Visa card online.

**Vkontakte** — This is Europe's largest social networking website, with more than 100 million users. It is most popular in Russia, Ukraine, Kazakhstan, Moldova and Belarus. Similar to Facebook, VKontakte allows users to message their friends privately or publicly, create groups and public pages, share and tag images and videos, and play games.

**WebMoney Transfer (WMT)** — This is a global bank settlement system and environment for online business activities, established in 1998. WMT originally targeted clients in Russia and the former Soviet Union, however, it is now used worldwide. The system enables internet users to conduct safe transactions in real time using WebMoney units (WM-units). No bank account or credit card is required to open or operate a WebMoney account. According to WebMoney, thousands of online shops and services accept WebMoney payments. WMT also provides online financial services, P2P payment solutions, internet based trading platforms, merchant services and online billing systems.

**Yandex.Money** — This is an online payment service. It is especially popular in Russia and describes itself as enabling users to pay anytime and anywhere for mobile services, internet, Skype, games, tickets, home utilities, and many other goods and services. Users can deposit money at bank branches, mobile retailers, payment kiosks, and other points, with most methods being omission free. [Yandex Payment Solution](#) is a universal tool for accepting payments online. Merchants can implement this Payment Solution to start accepting payments to a bank account by credit card and other popular methods.



SecureWorks

SecureWorks provides an early warning system for evolving cyber threats, enabling organizations to prevent, detect, rapidly respond to and predict cyber attacks. Combining unparalleled visibility into the global threat landscape and powered by the Counter Threat Platform — our advanced data analytics and insights engine — SecureWorks minimizes risk and delivers actionable, intelligence-driven security solutions for clients around the world.