Nightfall in Minsk means Dmitry Naskovets begins working the phone. At 24, Naskovets is tall and skinny, and still looks like the college kid he recently was. He’s in his apartment’s kitchen, in a respectable neighborhood off the second ring road in the capital of Belarus. He starts around 6 p.m. and usually doesn’t quit until three the next morning.

On this particular winter night in 2009, Naskovets checks the online orders that have come in and sees a routine assignment. A client has tried to buy a MacBook Pro online with a stolen credit card, but American Express blocked the purchase. Now it’s Naskovets’s job to work it out with Amex.

He calls the toll-free number, using software that makes it look as if he’s dialing from the U.S. Any information the customer rep might ask for, Naskovets’s client sends him instantly by chat. The questions don’t usually get beyond the cardholder’s date of birth, Social Security number, or mother’s maiden name, but the woman fielding this call is unusually thorough. She notices that the phone number on the account has changed recently, triggering extra security. She puts Naskovets on hold while a colleague dials the old number and gets the actual cardholder on the line.

Thus begins an absurd contest: Naskovets against the man he’s impersonating. The agents throw out questions to distinguish the fake. When did you buy your home? What color was the car you bought in 2004? Each time Amex puts him on hold, he knows the legitimate cardholder is being asked the same question. At last, the rep thanks him, apologizes, and approves the purchase.

Naskovets was even better than the real thing. (Amex declined to comment on the incident.)

Telling the anecdote years later, Naskovets is still amazed that Amex got it wrong. And he has a certain sympathy for the victim, who had to dredge up details from memory, while Naskovets just read off a screen. “This guy has his credit stolen from him in front of his eyes,” he says.

From 2007 to 2010, Naskovets was an identity thief—the voice on the phone that explained questionable purchases to banks and gave final approval for fraudulent wire transfers. He didn’t convince every agent; about a third of the time, the scam didn’t work, he says. Hang up, move on. But he was successful enough to smooth the way for more than 5,000 instances of fraud, according to the U.S. Department of Justice.

If a bank employee got suspicious, Naskovets feigned impatience. “I don’t have time for this!”
The prefix “cyber-” evokes technological sophistication, yet cybercrime depends on legions of old-fashioned crooks. They’re foot soldiers with no particular computer skills who play the part of customers over the phone or cash out compromised accounts and send laundered money to superiors in Eastern Europe or elsewhere. As data theft has exploded, with hackers vacuuming up hundreds of millions of credit card and bank account records in recent years, so has this service sector.

“I understand it’s bad,” Naskovets says. “I understand that. But in the beginning, when you’re sitting in Belarus, and you’re very young and you need money … ,” he trails off. “You don’t see blood, you don’t see crying people in front of you. You’re just pushing the button.”

Naskovets grew up in Borisov, a small city an hour northeast of Minsk, raised by his grandmother and his mother, a nurse. He attended a public school with an intensive English program, with lessons six times a week from age 6 to 15, including classes in literature and translation, then studied finance in college. At 22, he was working for a Minsk car dealership when he ran into a former classmate named Sergey Semashko on the subway. He mentioned a job opportunity for someone with excellent English.

A few days later, Naskovets visited Semashko, whom he’d never known to be wealthy, in a mysteriously high-end apartment in one of Minsk’s better neighborhoods. Semashko left the details of the job vague. Get a headset and a Skype account, he told Naskovets, handing him $500—more than Naskovets earned in a month.

Whatever this new chance might be, Naskovets had reasons beyond greed for jumping at it. Selling cars wasn’t the career he’d planned. When he graduated in 2004, he’d gotten a job at a state-owned bank. But after joining a demonstration that criticized President Aleksandr Lukashenko, he was detained by Belarusian security agents. (They’re known by the initials KGB, as in the former Soviet Union.) The agents wanted him to snitch on his fellow demonstrators, he says. He refused. The KGB persisted. When Naskovets stopped answering his personal phone, agents called him at the bank, and the bank didn’t renew his contract. Finding a job became difficult. The KGB kept up its pursuit, detained him again, and then pressured the adhesive tape factory where he’d found work to fire him, he says.

It was late 2006, and as Naskovets struggled, a golden age of cybercrime was underway. TJX Cos., the owner of T.J. Maxx and Marshalls stores, would shortly discover that hackers had made off with credit card data for 46 million customers—one of the first corporate megabreaches. Within a year, the Zeus Trojan, a piece of malware designed for bank robbery, would infect tens of thousands of computers. The new efficiency in harvesting stolen data created a bonanza of opportunities in the black market. This was the world Naskovets entered.

He set up an e-mail account, f.sinatra54@gmail.com, and began to get messages from strangers via Semashko. At first, they wanted him to check a credit card balance or change the billing address on an account. The requests quickly became more obviously illegal—impersonating bank customers and getting bogus wire transfers approved. To Naskovets, it felt almost like a game. “It’s crazy and every day something new,” he says. “You can do it from your kitchen in your underwear with a beer.”
By mid-2007, his business was thriving. Customers typically reached him via an order form on the website he and Semashko set up, CallService.biz. They advertised on CardingWorld.cc and other forums popular with data thieves.

His hacker partners did the complex computer work of stealing account data, logins, and passwords; Social Security numbers; and security questions and answers. They would then initiate fraudulent transfers or purchase expensive, easily resold items such as watches or Apple computers. With his conversational English, Naskovets provided the final piece, getting around the toughest security measures—if an outgoing wire required verbal confirmation, say, or a card company called to make sure it was really John Smith buying that $3,000 watch on EBay.

Naskovets did as many as 30 calls a day, charging about $20 a pop or a percentage of the transaction. For most jobs, customers provided the information he needed, usually culled from credit reports. If a bank asked for ID, Naskovets knew a guy who could e-mail a PDF of a fake driver’s license in seven minutes for $20. If he didn’t know the answer to a security question, or an agent got suspicious, he had a strategy: feign impatience or frustration. American financial institutions focus on customer service at the expense of security, Naskovets says. “Why are you asking me that?” he’d sputter. “I don’t have time for this! I need to get this done!”

His accent wasn’t much of a problem. Agents at banks followed a tight script. As long as he had all the answers right, he says, they weren’t going to risk going to a supervisor over a foreign accent.

Not that there weren’t hiccups. Once, when he was supposed to be someone named Thomas Jefferson, an agent pointedly asked if he knew who that was. He began to get threatening calls from bank security personnel and the FBI. “We’re going to get you,” they said. He’d tell them they had the wrong number.

He didn’t worry too much about those calls. He didn’t know who any of his clients were, and all they knew about him was his instant message account, or so he thought.

“It’s crazy and every day something new. You can do it from your kitchen in your underwear with a beer”

Naskovets is cagey about how much he brought in—sometimes $400 a day, sometimes $1,000, sometimes nothing. He avoided transactions involving millions of dollars, preferring smaller stakes, less anxiety, and greater freedom. “The bigger the money, the bigger the mental tension,” he says. Instead, he enjoyed himself. He could afford restaurants and nightclubs. He traveled for the first time, to Bulgaria, India, Paris, and Turkey. He married his girlfriend. “It was a good life,” he says. “The most important thing was a kind of freedom from anything.”

With his profits, he tried to start over outside Belarus. In 2009, Naskovets and his wife left for Prague with plans to start a pet supply store. But his old clients kept bringing him work. “I already understood I cannot do this business all my life,” he says. “It was so difficult to cancel—people are constantly messaging you.”
Naskovets was at home on April 15, 2010, in a six-story apartment building near Prague’s biggest park, when the power cut out. The doorbell rang; a man in a bright orange jacket with a company name on it waited outside—an electrician, Naskovets assumed. Naskovets opened the door and found a gun in his face. Shouting, the fake workman forced him to the floor, handcuffing him while more officers entered the apartment. A silent FBI agent stood watch. They put Naskovets in a chair and showed him a document. It said he could go to jail for 39½ years in the U.S. for conspiracy to commit wire fraud and aggravated identity theft. Then they bundled him off to Prague’s Pankrác prison, wearing a zip-up Fair Isle sweater and looking like an early ’60s Beatle with his floppy hair.

Belarus authorities arrested Semashko on the same day, and officials in Lithuania seized computers that hosted CallService.biz. Preet Bharara, the U.S. Attorney for the Southern District of New York, trumpeted the arrests: “Dmitry Naskovets’s website was essentially an online bazaar for dangerous identity thieves. ... Today, we have shut down that business and protected untold thousands of potential victims of identity theft.”

Naskovets didn’t know how the U.S. had found him. He suspected a former girlfriend had turned on him. Also, the indictment referenced a chat where he’d inadvertently sent personal information to a client. His first instinct was to fight the charges. He didn’t cooperate when U.S. authorities attempted to interrogate him in May 2010. But his lawyer told him to accept extradition and make a deal; by mid-September he was at the Metropolitan Correctional Center in Manhattan. He pleaded guilty in 2011. In March 2012, Judge Lewis Kaplan sentenced him to 33 months, most of which he’d already served, and ordered him to pay $200.

“I want to say thank you to the American government for giving me an opportunity to clean my hands in front of justice in such a humane and civilized way,” Naskovets told the judge, “for giving me the opportunity to accept responsibility for all unlawful and immoral deeds and to start a new part of my life with totally different ideas in my mind.”

He meant it. After a conversation with Naskovets, you realize quickly that he’s a relentless optimist. He paints his time in the U.S. correctional system as an adventure. “I get this philosophy probably from my grandmother. It’s like, ‘Life is good no matter what.’ ” He spent the biggest chunk of time in Brooklyn’s Metropolitan Detention Center, working a 3-to-8 a.m. kitchen shift for 20¢ an hour and reading—the New York Times, Keith Richards’s Life, and Russian novels donated to the prison library by a previous inmate, Ukrainian hacker Roman Vega. Cybercrime, Naskovets discovered, commanded respect. He got more than one business proposal from fellow inmates for work when he got out.

“You can get life for two kilos of cocaine, but if you’re going to get some bank fraud, OK, you’re going to get 18 months,” he says. “And at the same time, the reputation you got, it’s like, ‘Oh, you are the most sophisticated.’ So this is crazy.”

Factoring in time served and a reduction for good behavior, Naskovets got out in September 2012. He faced a deportation order that would have sent him back to Belarus. Representing himself in immigration court, he argued that he risked torture if sent home, based on his run-ins with the KGB. As a signatory to the U.N. Convention Against Torture, the U.S. cannot send
someone back to a country knowing he’s likely to be tortured. An immigration judge sided with Naskovets. The government appealed.

Here’s where Naskovets’s optimism proved justified. While he was buffing floors in a county prison in Pennsylvania, his case had caught the attention of Stephen Yale-Loehr, a law professor who runs an immigration clinic at Cornell. With the help of Yale-Loehr and his students, Naskovets fought Immigration and Customs Enforcement in court for two years—and in October 2014 the agency decided to let him stay.

I met Naskovets two weeks later, at a Central Asian restaurant near Coney Island. He already had a job, doing office work for Arkady Bukh, the lawyer who’d represented him in his criminal case. He ordered fried Russian dumplings and coffee. He looked rough, dressed all in black, with unkempt hair, a deep pallor, and teeth chipped in a prison accident. He more or less matched my mental image of an Eastern European identity thief.

By February 2015, Naskovets was living in Far Rockaway, Queens. He picked me up in a friend’s white Audi sedan, wearing a long black dress coat and new shoes, with new teeth and a haircut. He’d been taking an online course on the art business through Sotheby’s. He’d also applied for a Discover card. “From the professional point of view, I’m analyzing how they work,” he says, unimpressed. “They ask very secure, very tough questions—they think—like, ‘What is your business address?’ ”

Naskovets and Bukh have since started their own company, CyberSec, which bills itself as “a different kind of cyber security firm.” Their website touts the skills of “hackers who are now using their knowledge of computers to do good.” They include Igor Klopopov, who’s back in Russia after serving a sentence for identity theft in the U.S., and Vladislav Horohorin, formerly known as BadB, a notorious Russian hacker who’s still in jail in Massachusetts for credit card and wire fraud.

Not long after he got out of jail, Naskovets contacted the American Express security department to offer his help. “I was like, ‘Because of you, I’m here. I’m good, so let me pay you back a little bit,’ ” he says. The company didn’t take him up on the offer.
We explain the scams, how they work and ways to keep your money safe. ID fraud claimed more than 148k victims last year - a 57% annual rise. One couple had £8k stolen from their joint account by criminals. We explain all of the ways you can fall victim - and how to prevent it. Identity fraud. Criminals glean personal information about an individual to open accounts in their name, order a mobile phone contract, request other goods in their name or empty their current account. Investment fraud. Sometimes known as 'boiler room' fraud. The caller will suggest there is evidence of fraud on an account and recommend the person phones their bank's fraud department. When the account holder hangs up and dials the number, the original call is never disconnected. How do thieves steal an identity? Identity theft can start when someone gets and misuses your personal information such as your name and Social Security number, credit card number or other financial account information. The thieves might use a variety of methods to steal your information, including: Skimming: Stealing credit/debit card numbers by using a special device on ATMs or when processing a purchase. Phishing: Pretending to be a financial institution or other company and sending email or pop-up messages to get you to reveal your personal information. Notify all your banks and financial companies as soon as you realize your identity has been stolen or an account is at risk. If you bank with us, call us immediately. Thief, also known as Kreacher Pierson, is a default survivor unlocked after completion of the prologue. He is one of the 31 playable Survivors added to Identity V. Kreacher has a slim build with a peach skin tone. He has short brown hair, which extends to a beard that covers his lower face. He dons a white button-up shirt, a pair of brown pants, a pair of brown boots, a black tie, and a brown newsboy hat. With one blue button on his left eye and a brown button on his right, it is believed that he... From 2007 to 2010, Naskovets was an identity thief—the voice on the phone that explained questionable purchases to banks and gave final approval for fraudulent wire transfers. He didn’t convince every agent; about a third of the time, the scam didn’t work, he says. Hang up, move on. But he was successful enough to smooth the way for more than 5,000 instances of fraud, according to the U.S. Department of Justice. If a bank employee got suspicious, Naskovets feigned impatience. "I don't have time for this!" As data theft has exploded, with hackers vacuuming up hundreds of millions of credit card and bank account records in recent years, so has this service sector. "I understand it's bad," Naskovets says. "I understand that."