WIRED NEWS

I Was a Cybercrook for the FBI

For 18 tense months, a computer-savvy grifter named David Thomas runs a thriving online crime hub for bank heists, identity theft and counterfeiting, with the FBI paying the bills.

By Kim Zetter 02:00 AM Jan, 30, 2007

By the time David Thomas eased his Cadillac into the parking lot of an office complex in Issaquah, Washington, he already suspected the police were on to him.

An empty Crown Victoria in one of the parking spaces confirmed it. "That's heat right there," he told his two passengers -- 29-year-old girlfriend Bridget Trevino, and his crime partner Kim Marvin Taylor, a balding, middle-aged master of fake identities he'd met on the internet.

It was November 2002, and Thomas, then a 44-year-old Texan, was in Washington to collect more than \$30,000 in merchandise that a Ukrainian known as "Big Buyer" ordered from Outpost.com with stolen credit card numbers. His job was to collect the goods from a mail drop, fence them on eBay and wire the money to Russia, pocketing 40 percent of the take before moving to another city to repeat the scam.

But things didn't go as planned.

Ignoring Thomas' suspicions, Taylor walked into the Meadow Creek Professional Center to collect the Outpost shipment, and found the cops waiting for him. Thomas and his girlfriend tried to escape in the Cadillac but were caught half a mile away.

An ID badge that Taylor wore when he was arrested indicated that he worked for Microsoft. But that was no more accurate than the two-dozen other employee badges he possessed for E-Trade and AT&T Broadband, or the 15 driver's licenses from various states that featured his congenial face and a dozen aliases. Nor did Thomas' California driver's license help authorities identify him. Although it had his picture, the name and address on the ID belonged to a producer for the A&E channel.

With so many fake IDs in play it was unclear to police exactly who they had in custody. Then as they read Thomas his rights, he told them: "Get me some federal agents and I'll give you a case involving the Russians and millions of dollars."

Thus was the beginning of Thomas' turn to the other side. For 18 months beginning in April 2003, Thomas worked as a "paid asset" for the FBI running a website for identity



- 1 -

and credit card thieves from a government-supplied apartment in the tony Queen Anne neighborhood of Seattle.

From bedrise to bedrest, seven days a week, he rode the boards and forums of his and other carding sites using the online nickname El Mariachi. He recorded private messages and IRC chats for the FBI as "carders" schemed to, among other things, sell stolen credit and debit card numbers, defraud the George Bush and John Kerry campaign sites, drain hundreds of thousands of dollars from bank and investment accounts, sell access to Paris Hilton's T-Mobile account and run phishing scams against U.S. Bank and the FDIC. He did it all while battling denial-of-service attacks against his site and dodging attempts by his old partner Taylor and other carders to track his whereabouts and out him as a fed.

Just as his enemies were closing in on him in September 2004, the FBI pulled the plug on his work and cut him loose. But not before Thomas had given authorities a valuable look at the internet's underworld, even though the strain of leading a double life nearly broke him.

Now Thomas is telling the story of his work during this period. It's a tale that provides a rare glimpse of the thriving international computer underground of high and low-tech thieves and swindlers whose crimes cost millions each year. It also illuminates the rarely seen world of federal law enforcement's war against these organized criminals, and the moral and ethical tradeoffs sworn agents make in pursuing their mission -- providing crooks with an electronic marketplace where they can congregate and conduct their

ignominious business anonymously. Even allowing some crimes to go unpunished.

The full scope of the problem is hard to judge, but nonetheless staggering. U.S. banks lost \$546 million to debit card fraud in 2004, according to banking research firm Dove Consulting, and credit card fraud losses were estimated to be about \$3.8 billion globally in 2003 according to The Nilson Report. The Federal Trade Commission estimates that 10 million



Americans are victims of identity theft each year. The financial impact of identity theft remains untold.

Thomas says he is telling his story now because he's tired of the life he's lived on the boards over the last five years and resentful of the control the FBI maintained over him for so long. He also wants to warn the public about the risks they face from the carding community and deter kids from being seduced into a life of crime.

The FBI's Seattle office wouldn't discuss Thomas, and neither confirmed nor denied that he worked for them. But over the last year Wired News verified other key aspects of Thomas' account in dozens of interviews with members of the underground, victims of



- 2 -

online crimes he observed, as well as attorneys and other people connected with Thomas -- his former apartment manager, for example, confirmed that the FBI paid Thomas' rent.

Additionally, Thomas provided hundreds of chat logs and forum posts from his former website, The Grifters ¹ -- a criminal marketplace that played a key role in a parade of diverse frauds, ranging from bank theft to telephone records hacking, all unfolding in a sprawling international tableau spanning from the former Soviet empire to the tropics of Colombia.

It was July 2004 and Brian Campbell had been on Isla Mujeres off the coast of Cancun for three days for a relative's wedding when he discovered he'd been scammed.

An American MBA student studying in Australia at the time, Campbell (not his real name²) was accustomed to checking his investment portfolio daily over the internet. But the wedding distracted him a couple of days, and when he finally got online, he found he was locked out of his Schwab trading account.

He called Schwab and discovered that his user name and password had been changed. What's more, \$106,000 had recently been wired from his account to a Fortis bank account in Belgium. Campbell hadn't requested the transfer.

Unknown to Campbell, a cyber thief who went by the nick "desertmack" had gained access to his e-mail account and had been watching him for weeks. The Mexico wedding was the break desertmack needed. He'd been hoping a little tequila and sunshine would distract Campbell from obsessively checking his brokerage account long enough to steal the money and send it to Brussels, where an accomplice would withdraw it.

But while desertmack was watching Campbell, the FBI was watching him. Or at least David Thomas was. Sitting in a 500-square-foot Seattle apartment, window shades drawn and cramped with three computers that emitted an oppressive heat, Thomas recorded every conversation that desertmack and his accomplice, who used the nick jonjacob, exchanged in a private area of TheGrifters.net.

TheGrifters was a members-only "carding" site that Thomas launched in December 2003, eight months after beginning his work for the FBI. The goal of the site was to attract identity and bank thieves. It was the kind of site authorities called a "build it and they will come" site. And they did.

By mid-2004 the site was crawling with thieves trafficking in fake IDs, stolen credit card numbers, card-embossing equipment and ATM skimmers that capture data on a debit card's magnetic stripe so criminals can encode it on blank cards and drain an account. TheGrifters was a successful crime hub in a crowded field, competing with other sites like Shadowcrew, CarderPlanet and DarkProfits to attract the biggest criminals.

None of the carders knew that Thomas was working for law enforcement, although there were many who accused him of it. Indeed, if a carder was arrested and returned to the

- 3 -



boards, as Thomas had done, often he *was* working for "LE," in carder lingo. But the boards were always thick with a fog of police paranoia, and no one took the accusations seriously enough to stay away from Thomas.

Thomas began following desertmack closely after he saw the crook purchase a credit report for Campbell from a Florida woman who used the nick Decepgal. Decep ran a carding site called Muzzfuzz and, according to bankruptcy filings in her real name, worked as a transcriber of psychiatrists' notes. She also ran a side business selling credit reports to identity thieves -- \$40 for a standard report or \$75 for full-info reports that included a victim's property holdings, bankruptcy filings and lists of possible relatives³

The report, coupled with e-mail account statements, gave desertmack all he needed to access Campbell's Schwab account and initiate the money transfer. Jonjacob and another associate in Brussels then opened a Fortis business account -- chosen because of the bank's \$40,000-a-day withdrawal limit on such accounts. As the day for the transfer neared, the thieves could hardly contain their excitement: "Hehe, fingers firmly crossed, along with my legs, testicles and anything else I can think of," one associate wrote desertmack.

Then, on the day of the theft: "well ... I expect our friends are off enjoying their holiday. And with a bit of luck, you're busy raping that juicy account of theirs."

The night before the attack, desertmack changed the contact number on Campbell's account so Schwab would call him for verification instead of Campbell if it suspected the wire request was fraudulent. The ruse worked. Within 24 hours the money was on its way to Brussels. But that was the last desertmack heard of it. Once the funds were overseas, his accomplice jonjacob disappeared.

If desertmack suspected a double-cross, he was wrong. Campbell, who confirmed the details of the theft for Wired News, learned from Schwab that a suspect was arrested in Brussels while trying to withdraw money from Fortis.⁴)

Shortly after that, it appears that desertmack was arrested too, though not for the Schwab crime. Oregon sheriffs arrested a 47-year-old man on unrelated identity theft charges in September 2004, after his wife was involved in a car accident and deputies discovered outstanding warrants on both of them for an old eBay fraud caper.

Police searching the couple's apartment found equipment for making credit cards and fake IDs, as well as 432 stolen credit card numbers, 176 bank account and routing numbers and boxes of credit reports in other people's names. E-mail found in the suspect's computer inbox was addressed to desertmack@mailvault.com.

"He was very organized," Oregon deputy sheriff David Thompson told Wired News. He had 510 dossiers on victims that consisted of "each person's credit cards and IDs that he had created, bundled up with a rubber band so that he could just grab a bundle and have



that identity for a day to go out and go shopping." The suspect claimed it was all research for a book he was writing about fraud prevention.

Oregon FBI spokeswoman Beth Ann Steele said the man was suspected of initiating the Schwab wire transfer, but said the bureau didn't pursue charges because local authorities had a stronger identity theft case against him.

The Schwab case illustrates a running theme in Thomas' dealings with the FBI. Although Thomas says he provided his handlers at the Seattle FBI with logs depicting desertmack's scheme, the bureau apparently never acted on that information -- the Oregon FBI only learned of the theft because Campbell, the victim, reported it himself after it occurred. "If we had left it up to Schwab, they might never have gotten the FBI involved at all," Campbell says⁵,

Schwab, too, was less than responsive. Campbell got his money back from the company only after several calls to the firm pointing out the obvious security flaws in a system that failed to flag a wire request made on an account a day after contact information on the account was changed. "Schwab was pretty bad with customer service," Campbell says. "For a long time they wouldn't tell me they were going to take responsibility for it and return (the money)." (Schwab had no comment).

As for Thomas, he was unaware of desertmack's fate until Wired News tracked down the suspect. As with all of the information Thomas provided the FBI, he was kept in the dark and never knew what, if anything, the agency did with the intelligence he gave his handler.

Thomas began his work for the FBI five months after his Issaquah arrest and after serving three months in jail. His partner, Kim Marvin Taylor, known by the nick "Macgyver," left Washington before he could be charged, and landed quickly back on Shadowcrew, where he was a top administrator of the site.

After Thomas' arrest, federal agents came to see him in jail, as he'd requested. He told Secret Service agent Michael Levin what he'd done for the Russians, but Levin wasn't impressed. According to Thomas, the agent replied that he had multi-million-dollar cases on his desk and wasn't going to waste time on a lousy \$50,000 internet scam.

Seattle FBI Agent Steve Butler also came to see him and seemed just as unresponsive at first. The jailhouse chat through a glass partition lasted less than 10 minutes with no mention of a job. But when Thomas was transferred to Nebraska to face an outstanding warrant for check fraud, Butler showed up for a repeat visit, an assistant U.S. attorney in tow.

The agent laid out his plan: Thomas would work for the Northwest Cyber Crimes Task Force in Seattle to gather intelligence and teach Butler how the carding sites operated; in return, the FBI would pay his rent and all of his expenses. It would be an intelligence gathering mission, not aimed at making arrests, but rather at learning how the international carding scene operated.

"They made a big show down there," Thomas says. "They told me that they'd take care of me, and I'd have a legit job with them."⁶.

He didn't have to think twice. No one had ever sought him out for work before, and in an age of background checks they likely wouldn't. But that wasn't the only reason he took the offer. He wanted to write a book about the carding world, and figured this was the perfect chance to gather material. "(The FBI) wanted to see just what they could get out of it, and I wanted to see what was really going on and to write about it," Thomas says. "It was a win-win situation."⁷.

His lawyer got the Nebraska charges reduced to a misdemeanor and fine, and by April 2003 Thomas was back in Seattle, where girlfriend Trevino joined him, and on the boards, using computers the FBI supplied him.

But almost immediately the words he'd spoken in Issaquah came back to bite him. On CarderPlanet, someone posted a copy of his police report containing the statement he made to police about the Russians and federal agents. Taylor, still a fugitive, took to the boards and accused Thomas of selling him out to the feds. A war of words broke out between Thomas' supporters on CarderPlanet and Taylor's supporters at Shadowcrew.

"All of a sudden, whatever I was hired to do (for the FBI) looked like I wasn't going to be able to do it," Thomas says. "In my mind I was toast. Because that report was too damning."

Thomas denied the claims to little avail. Then, two months later Taylor was jailed in Colorado on new charges unrelated to the Issaquah bust. He served eleven months before being released in May 2004.

But his absence did little to foster calm. Over the next year, the board war would escalate from verbal scuffling to all-out Joe Jobs and DDoS attacks. And every 45 days or so when things would quiet down, someone would repost Thomas' police report to stir them up again.

Between battling other carders and gathering information for the feds, Thomas' workdays were long and full of non-stop activity.

He became obsessed with knowing everything that was happening on the boards. He'd often sleep during the day, then work all night when the boards were most active. Each day when he awoke, he'd hop on the boards to see what had happened while he'd slept. Were any carding sites down? Had anyone been arrested? Then he'd run through a checklist of scams unfolding that day. He spent 18 to 20 hours a day online with 15 to 20 chat windows open on his screen at a time. When he wasn't chatting online, he was talking on the phone.



"People would talk to me -- I've got this deal, I've got that deal. What do you think of this, what do you think of that?" he says. "El had a huge following."

His job was to log every message he received and sent as well as every note that members posted to the boards. At the end of each day he sent Butler a report. Sometimes there were more than 300 messages in a single discussion thread. Every morning Butler debriefed him by phone, and once a week they met in person. Everything he recorded for the FBI, he recorded for himself as well.

His task for the FBI was to track who was doing what, which wasn't always easy since members changed their nicks often and used anonymous e-mail, proxy servers and prepaid cell phones to mask their identities and whereabouts. Occasionally, however, they'd let their guard down. Thomas never pressed for details. But like a good psychiatrist, he did the cyber equivalent of nodding with interest, and people were happy to talk.

Ironically, even though the carders constantly accused each other of working for the feds, they often acted as if a cloak of invisibility shielded them. Larry Johnson, special agent for the Secret Service's investigative division who headed an undercover operation for his agency on the boards, says agents were often dumbfounded by the carders' lack of discretion. "If I were going undercover they would accuse me, accuse me and accuse me (of being a fed) and then buy something from me (anyway)," he says. "Figure that out."

Thomas says the carders believed they operated in a protected world. "It was all some fantasy criminal paradise," he says. "Nobody believed law enforcement was out there in force."

In truth, law enforcement agents were (and still are) some of the fraud sites' most determined users, and it wasn't just undercover U.S. feds scouring the boards. There were also agents from Russia, the U.K., Australia, Israel and Brazil. Fraud investigators from Visa, Bank of America, eBay and others also lurked on the sites, determined to gather intelligence about threats to their customers.

The presence of so many watchers meant that authorities sometimes targeted the wrong person for investigation. Although U.S. agencies held deconfliction meetings to apprise each other of who was doing what, word didn't always get around. When Thomas once asked Butler who was the biggest target the feds were tracking, Butler laughed and replied, "You're the biggest target. Everyone is after you."

Although the Seattle neighborhood where Thomas lived was upscale, his apartment was strictly low-rent. Except for a small couch and TV, the only living room furniture was an Ikea table that groaned from the weight of two desktop computers -- one for watching the boards and chatting with carders, the other later used for hosting TheGrifters -- and a laptop for compiling reports to Butler. Trevino occasionally helped out with research but for the most part avoided Thomas' work and spent her time chatting with friends online and playing digital games.

"I didn't want to be there doing what he was doing," Trevino says. "I didn't want to be a part of it. Because I had done my time (in the carding community) and I didn't want to do any more."

To conduct his work, Thomas was allowed to facilitate and commit crimes, but only after clearing them with Butler. Butler said undercover agents from other agencies who didn't know what Thomas was up to would try to set him up, and Butler would need to run interference when he saw it happening. He was also told that if he committed any crimes without clearing them first, Butler would make sure that he went to prison, and that other inmates would know he'd worked for the FBI.⁸.

The boards had a strict hierarchy that Thomas had little trouble infiltrating. At the top were administrators, like Taylor, who handled day-to-day operations and served as gatekeepers to private areas of the board where the best deals were made. Admins also meted out punishment to carders they didn't like or to "rippers" who cheated fellow carders.

An admin could ban someone from the board or, worse, post his photo online and expose his identity. The pictures came from fake-ID vendors who often held on to the photos of customers just to use them when someone got out of line.

Beneath the admins were moderators who oversaw forums dedicated to various topics, such as bank fraud and identity theft. Then came vendors and reviewers. Before a vendor could sell his merchandise on the boards, a reviewer evaluated the quality of his offerings based on such criteria as the quality of a hologram on a fake ID, or whether the stolen credit card numbers a vendor was hawking were still live and valid. Most reviews consisted of a couple of lines: "Cards good. Premium numbers with high balances."

The organized chain of command allowed a rich economy to flourish -- and the range of products and services at offer was staggering. While credit card fraud was a staple of the cyber underground, a wide variety of other crimes also unfolded -- and still unfold -- on the boards. Some underground denizens offered spamming and "bullet-proof" hosting services from servers placed in locations unreachable by law enforcement. Extortionists used botnets to deliver DDoS attacks against websites that didn't pay protection money. And hackers designed and sold rootkits, spyware and spam mailers, alongside peddlers of stolen source code from companies like Microsoft. Pretty much anything went in the underground if it could produce a profit.

Of course, the quickest way to make money was to, literally, make money. And when a Colombian counterfeiter named Dexer showed up on the boards peddling top-quality fake dollars and euros, Thomas was interested.

After consulting with Butler, Thomas asked Dexer to send him some sample bills to review their quality. Two weeks later they arrived at an FBI mail drop in Seattle, secreted in a hollowed-out book cover.

Although Thomas never saw the bills, Butler told him the counterfeiters had bleached \$1 and \$5 bills then printed \$50 and \$100 denominations onto the paper to produce nearperfect fakes. Thomas gave Dexer a glowing review on CarderPlanet, and orders began pouring in -- that is, until members started complaining that bills they ordered never arrived. Dexer said U.S. customs was holding them up. He discussed plans to get around the blockade, but shortly thereafter his nick disappeared from the boards, leading others to wonder whether he'd been arrested or simply skipped out to avoid the anger of dissatisfied customers who never received their bills.

Did the FBI move in on Dexer? As usual, Butler kept Thomas in the dark. The uneven power relationship between Thomas and his handler, and the increasing claustrophobic nature of Thomas' life, took their toll over time. The strain wasn't helped by the differences in Thomas' and Butler's personalities.

As Trevino describes him, Butler was the polar opposite of Thomas -- tall and confident with tightly cropped blond hair and the physique and jaw of a college jock. According to Thomas, Butler's background was in drug investigations not cyber crime, and the two of them frequently butted heads over how to run the operation, often resulting in shouting matches in Butler's car as they drove around the neighborhood for their debriefing sessions.

"He was very intelligent," Thomas says. "But ... we just never hit it off."

The conflict came to a head one day after Butler rebuffed Thomas' requests for some time off to get some rest. When Butler next phoned for their routine debriefing session, Thomas, exhausted, refused. "I'm on vacation."

Another shouting match ensued, culminating in Butler coming to the apartment and carting off the computer Thomas used to host TheGrifters website. As Butler left with the PC, he told Thomas he was fired and gave him a week to leave the apartment. Dumbfounded, Thomas sat there for days struggling to figure out where he'd go with no money when Butler, his point finally made, called back. "Okay. Are you ready to get back to work now?"

When TheGrifters went back online Thomas had to cover for his downtime by telling board members he'd been taken out by a DDoS attack.

The troubles with Butler were only compounded by the continuing attacks that Thomas faced from enemy carders trying to expose him and take out his site. To deal with the stress of maintaining his double identity and battling Butler, he'd often retreat to the bathroom where he'd turn on the shower and lie on the floor, letting the water run for hours to clear the chatter from his head.

The shower ran so long one month that the FBI got a bill for 18,000 gallons of water. Thomas says federal investigators appeared at his door to see if he was growing marijuana or making homebrew. "They opened a federal investigation to find out where



- 9 -

the water went," Thomas says laughing. "And the water went down the drain. Because it was my only way to relax."

David Thomas' entrée to online crime came through the conventional world of offline crime. He was born to a Texas oil family, but this circumstance did little to grease his way through life. His parents divorced when he was four, and his father, a geologist and oil prospector, walked out of his life and died destitute in 1987, leaving Thomas with nothing more than a small oil royalty on a barren tract of Texas land.

Left to his own devices, Thomas gravitated to trouble. At 14, he stole a car -- his first felony; by 30 he'd been arrested several times for check fraud, forgery and burglary.

In the 1980s, it looked like things were turning around for him after he married, had kids and caught the computing wave, launching a business building PCs. But his climb up from crime didn't last long.

In 1993 he was working for a Texas company contracted to install electronic key-card systems in Doubletree hotels when Thomas thought his employer was mistreating Doubletree and convinced the hotel to give him the \$250,000-a-year contract instead. He was sure it would lead to other contracts. But he'd also just bought a new home in a gated community and needed money for the mortgage. So he bought cheap parts and overcharged Doubletree to get quick cash -- a bad choice made worse by the fact that the components were faulty.

He worked overtime to install the first system in Doubletree's Kansas City hotel then turned his phone off to rest. As luck had it, those were the days President Clinton's advance team were in town and staying at the hotel. When the key system failed, they were locked out of their rooms. Thomas turned his phone on a few days later to a series of shrill messages from the hotel manager. "Where are you? The computers are crashed, what are we going to do?!" Then: "You bastard! You son of a bitch! You'll never work in this town again!"

Thomas lost his house and marriage, and over the next decade alternated between legitimate and criminal work, none of it very successful. He got a job installing databases, then got fired when the company discovered he was on probation for check fraud. Then he smuggled marijuana across the Mexican border. After that more check fraud followed.

In 1998, at 40, he met Bridget Trevino on an IRC channel -- she was 25 and living with her mother. They crisscrossed the country for a year, living on money from relatives and forged checks. It was the perfect match. "We never argued. We both liked the same exact kind of life -- you know, quiet, sedate, white-picket fence," he says with no hint of irony.

Their vehicle broke down in the Midwest in November 1999, and two weeks later Thomas got a phone call, and a rare lucky break. The Texas land his father left him turned out to have oil and gas reserves beneath it. Big royalty checks started rolling in --



- 10 -

first \$2,000 a month, then \$6,000 and \$8,000. Thomas vowed never to return to crime, and for a year and a half the vow stuck. Then the oil flow slowed, and the checks dropped back to \$2,000 then \$1,500.

Fearing the well was about to run dry, he sold his royalties on Energynet.com, an auction site where the wealthy traded oil and gas royalties, and got \$70,000 -- enough for a down payment on a ranch house. But after six months the money and house were gone. "I never thought things would go south on me like they did. At that point I was bitter," he says.

He turned to his old standby, check fraud; but with outstanding warrants, he needed a new identity. That's how he found Counterfeit Library, a British website where vendors sold "novelty" IDs -- fake IDs that were the stock-in-trade of identity thieves. The site was "total nirvana for a criminal," Thomas says, and a revelation.

Thomas had used fake IDs before, but they wouldn't stand up to scrutiny in bright light. Counterfeit Library IDs, by contrast, were genius, with holograms and magnetic stripes. For \$150 you could buy any ID you wanted -- military, federal employee, even the FBI or Secret Service. A little more would get you the whole "rebirth package": birth certificate, driver's license, passport, Social Security card, employee badge (name your dream job), even utility bills to establish proof of residency.

There was also a service called PhantomInfo, which consisted of a script that tapped into the computers of the ChoicePoint data broker. For \$29 a month you could send unlimited e-mails to phantominfo@xanon.net containing the names of victims whose identity you wanted to steal; the program would search ChoicePoint's database and reply with the victim's Social Security number and current address.

"Today, it's just normal, everyday stuff," Thomas says. "But back then it was the first that we had seen of that kind."

This was the start of something big. A small number of carders had long exchanged stolen identity information and credit card numbers on electronic bulletin boards and IRC channels. But websites like Counterfeit Library launched a whole new era of white-collar crime, lowering the entrance barrier for those who never would have found such information otherwise, and creating a global market for trading in large amounts of hacked data. For the first time, crooks could specialize in criminal niches, and market that expertise to thousands of collaborators across borders.

In addition to fake IDs, Counterfeit Library had forums where members traded in special deals. But to participate in the best deals you had to be a senior member, and to be a senior member you had to have 1,000 posts to your name. So, adopting the online nickname "El Mariachi," Thomas set out to make 30 posts a day, aiming for senior status in five weeks.

Thomas wrote quality content that got him noticed. He wrote tutorials on bank fraud --"\$30,000 on a \$3,000 Investment" and "Payroll Checks for Fun and Profit" -- as well as



- 11 -

long, introspective pieces about a hard life lived and lessons learned. The piece that got him the most attention was a solemn meditation on karmic retribution, which he wrote after he and Trevino found the windows of their Cadillac vandalized while they were out passing bad checks. "We were out doing wrong things," he says, "and it was our time to pay the price."

He developed a following on the boards among older members who considered him a fellow traveler on the hard-luck path, and younger ones who were glad to get a fatherly ear in the quiet hours after midnight. The positive feedback was a drug to Thomas. He loved leaving the weak David behind and taking on a new persona. Where David Thomas was insecure, El Mariachi was confident and worldly. Where David was unsuccessful at crime, El was a master con man. On the boards, all his neuroses seemed to disappear.

"El is the key to the strength that I have," Thomas says. "I know it sounds psychotic . . . but that is the boards. The characters are built around people who have low self-esteem, and they're looking on the boards for whatever they're missing in life."

But Counterfeit Library was soon supplanted by a new and vigorous type of online criminal marketplace, led by the arrival of the Eastern European fraud merchants.

Eastern Europe, particularly Russia, Ukraine and Romania, has become a wellspring of internet crime in recent years -- a result of rampant corruption, economic decline and too many young hackers with sophisticated skills and a dearth of legitimate opportunity. Organized crime mobs from these countries have joined forces with hackers and become adept at crafting and carrying out online attacks of varying sophistication: from simple phishing ruses to active database intrusions. "Because organized crime is so well-entrenched there, and tolerated by authorities to some extent, they're the one who are moving into it most aggressively," says James Lewis, a senior fellow at the Center for Strategic and International Studies.

It's only natural that the bank-card system would draw their attention.

"It was the Russians who ... brought plastic online," Thomas says. "They had manufacturing facilities to manufacture credit card plastic and put data on it, and guys on the English side were like, 'Whoa!""

The "Russians" included two twenty-something Ukrainians named Dmitry Golubov and Pavel Chistov who, according to law enforcement officials, joined with 150 other Eastern European criminals in convening a summit at an Odessa restaurant in the spring of 2001. The result was CarderPlanet, a highly organized online carding and money-laundering emporium that set the standard for all carding sites that followed.

According to Thomas, Golubov, aka "Script," was a spammer who realized the potential for carding when he saw how easily people sent their credit card numbers through e-mail to purchase the products he hawked. His group of cohorts paid hackers \$1,000 a day and more to crack bank and card-processing databases to steal credit card numbers, which



- 12 -

they sold in "dumps" of hundreds of numbers online. They set up botnets to spam out phishing lures, and even created a makeshift factory for manufacturing blank plastic cards with magnetic stripes and holograms. When Russian authorities eventually raided their workshop in June 2003, they found 8,000 counterfeit credit cards, according to an article in *Pravda*.

CarderPlanet's how-to tutorials and message boards became a daily must-read for criminals looking to make their mark in the burgeoning field of cybercrime. As one Russian carder noted in a message on the site: "Some people read '*Kommersant*', others '*Pravda*,' but we -- Planet."

"They were advancing crime by leaps and bounds," Thomas says. "It was a 24/7 operation that never slept."

Where the Russians went, everyone else followed. Although CarderPlanet was initially exclusive to Eastern Europeans, the site later added an English-speaking forum to attract partners in the United States and Britain who could cash out ATM cards and run drop addresses for stolen goods.

The site eventually amassed 7,000 members, according to authorities, about 450 of whom overlapped with an increasingly popular U.S. site called Shadowcrew.

"When Shadowcrew first came up and people made a \$5,000 score, people were like 'Wow, you're big time," Thomas says. "But later on ... guys were making \$100,000 a day."

A former Irish carder who used the nick "ITR" told Wired News in an e-mail that the amount of cash he pulled in from his carding days was, at times, hard to keep up with. When asked how much he stole, he replied, "Above the national average, and with some decent investment life is good."

Thomas, of course, wanted in on the action. It wasn't long before he hooked up with a Ukrainian man named "Big Buyer," one of the top Eastern European carders, whose nick derived from his penchant for maxing out stolen credit card numbers with big-ticket items, such as \$30,000 watches. "If he had \$50 left on the card, he'd go find another item to max out the card," Thomas says.⁹

Thomas went to Seattle where he began laundering money and receiving and selling merchandise for Big Buyer.

But carding wasn't his ultimate goal. Thomas had bigger plans in mind. He was devising a scheme to defraud traders at Energynet.com, the auction site where he'd sold his father's oil rights. He needed money from the Big Buyer operations to establish himself as a player at Energynet, where he planned to sell \$5 million in oil and gas royalties that didn't exist.

- 13 -



The "Rockford op," as he dubbed it in honor of James Garner's character in *The Rockford Files*, would be his final scam, the swan song every grifter dreams of that would allow him to retire from a 30-year mediocre career in crime that he no longer had the stomach to pursue.

But it was not to happen. Thomas was on the carding sites only five months before he and Taylor were arrested in Issaquah, Washington, and he began his new role for the FBI.

"I'd like to screw this guy, but it's not my field," a carder using the name "BoBaBc" wrote on CarderPlanet a few months after Thomas started work for the FBI. "If you can help me set it up we'll split it."

Some aspects of online fraud are seasonal -- in December, consumers are likely to receive malicious software crafted as electronic Christmas cards, for example. In 2004, the upcoming national election was looming large in America's consciousness, and cybercrooks like BoBaBc were looking for ways to cash in.

BoBaBc told Thomas he'd planted Trojan horses on the home computer of Darryl Tattrie, then a comptroller for the Kentucky Democratic Party. The hacker found numerous financial files on the computer, among them a spreadsheet listing donations to the party coffers, a list of bank account numbers with the names of people authorized to use them, and even a digital copy of Tattrie's signature for printing checks.

The fraudster had a plan to funnel \$250,000 from the party's campaign fund to an offshore bank account, and frame Tattrie for embezzlement. But he was a newbie to wire transfers and needed Thomas' help. Thomas tutored him for several days, and helped him compose a fax to the party's bank. But, of course, he was working both sides. When BoBaBc's anonymous cell phone broke, Thomas sent him a new one -- courtesy of the FBI. Thomas assumes the phone was under surveillance.

It's unclear how BoBaBc's scheme played out in the end. Around the time that BoBaBc intended to send the fax, he disappeared from the boards, and Thomas never heard from him again.

Tattrie, who now works for the Arizona Democratic Party, said that authorities spoke with him about the hack, but wouldn't elaborate on what agency was involved or what was said. It appears, though, that BoBaBc never made good on his embezzlement threat. Officials at the Kentucky Democratic Party and the party's bank say they never received the wire transfer request.¹⁰

BoBaBc wasn't completely idle, though. Around the time that he was purportedly planning his attack on the party's coffers, Tattrie returned from a trip to find that someone had transferred \$6,000 from his personal bank account. His ISP had also canceled his internet service on grounds that someone had been using his account to distribute spam while he was away.



The Kentucky Democratic Party wasn't the only political group targeted by carders that year. As the presidential campaign heated up, there were other schemes surfacing.

One carder using the nicks "Mesh" and "Nasa" decided to phish the Ralph Nader campaign site.¹¹ According to chat logs of his discussions with Thomas, he paid a coder to create a phony Nader campaign page that charged the donor's credit card and, cleverly, delivered the funds to the campaign, while simultaneously sending the card info to him.

When the scammer told Thomas what he was doing, Thomas joked that he should phish the Bush campaign site, too. So the scammer complied.

These were heady times for Thomas. He applied himself more diligently to his new job for the FBI than he ever had to other jobs, or even to his life of crime. In some ways it was the best of both worlds for him. He could spend his days immersed in the activities of the community he loved, scheming to commit crimes, without having to worry about being arrested. Of course, he didn't make money from his capers, but the thrill of being back in the game as El Mariachi and being in the know about what was happening on the boards made up for that.

Then in December 2003, Thomas' online war with other carders crossed a line and he found himself banned from some of the sites. That's when he decided to launch TheGrifters.net and become his own site administrator. The ban turned out to be a blessing: As the owner of his site, he now had unfettered access to all communication on the board.

On the surface, it seems remarkable that the FBI would finance and run an operation like TheGrifters, which facilitated crimes that inflicted very real financial losses against innocent consumers, merchants and banks. But Department of Justice guidelines allow the bureau to run long-term "criminal intelligence" investigations like the one Thomas describes, with no specific arrests or prosecutions anticipated, provided the target is a terrorist group or a "racketeering enterprise." The latter could clearly describe the community that immediately began gathering at TheGrifters.

Thomas had barely launched the site when he made his biggest catch, a Russian spammer who used the nick "King Arthur" and was one of the pioneers of phishing attacks. King kept a fairly low profile on the boards and avoided much of the drama and fighting that American carders were becoming known for. He had a much-coveted program for generating bank algorithms that would authenticate debit and credit cards to an ATM.¹²

What he didn't have was language skills. He wanted to steal money from customers of Minneapolis-based U.S. Bank, which boasts nearly 2,500 branches and 5,000 ATMs in 24 states. But he needed a native English speaker to author a phishing e-mail that could fool Americans into relinquishing their account and PIN numbers. That's where Thomas came in.

U.S. Bank was targeted because some of its accounts allowed \$2,000 or more in daily ATM withdrawals. A thief could withdraw two grand from an account at 5:59 p.m. one day and get another two grand at 6:01 p.m. -- the time when U.S. Bank ATMs reset themselves for the next business day.

Butler approved the operation, Thomas says, because phishing attacks were just coming onto the scene and he wanted to see how they operated. Thomas also thinks Butler was hungry for a big scam.

"(Butler) never wanted to work small cases," Thomas says. "He said, 'Look, if I get involved in an investigation or doing an intelligence deal and it's all simple time, I'd be working small time for the rest of my life.... I'm only doing the big stuff."

Today, according to some published reports, phishing attacks average 17,000 a month, with no sign of abating. But in early 2004, most people hadn't heard of phishing yet and were easily fooled by the scams. So when King sent out his phishing attack, it wasn't long before account and PIN numbers were rolling in, some with balances exceeding \$100,000.

Thomas was in charge of finding cashers for those accounts who wouldn't "rip." It was a common problem with ATM cashers. "You send a guy out to an ATM, he's going to be honest the first time or two out, and then he's going to start dipping in," Thomas says.

It was easy to claim that a card number hadn't worked, then pocket the cash. That is, unless you worked with Russian carders, who often claimed to have online access to the compromised bank accounts and knew exactly how much money a casher withdrew.

Thomas sent the numbers to a guy who used the nick "Myth," who coded them to blank cards and doled them out to 25 cashers across the country. Their job was to move from city to city hitting ATMs. Among the cashers were "Decep" and "John Dillinger," a carder who described his cashing activities to Wired News earlier this year before he was arrested.¹³ Decep claimed to pull \$11,600 from nine cards one night. Myth got \$90,000 in a few days, according to Thomas¹⁴.

The cashers wired 80 percent of their take to King in Russia through Western Union, while Thomas tracked card numbers and amounts on a spreadsheet and kept copies of ATM receipts, which the cashers were required to scan.¹⁵ As far as Thomas was concerned, it was all about keeping King happy. If Thomas got labeled a ripper, King and others wouldn't do business with him, and then he'd lose his value to the FBI. Every six months Thomas says the FBI rebudgeted for his surveillance work, and he was always worried that Butler would pull the plug if he didn't prove his worth.

"The thing you have to fight, that you're always fighting, is the diminishing value curve," Thomas says. "If you did really good last month and this month you're shit, you're already a diminishing value."

Throughout all of this, Thomas actively participated in King Arthur's schemes without FBI interference, despite the impact on banks and consumers. Although federal law requires that banks absorb such fraud losses, consumers are still left with the burden of reporting missing funds in a timely manner and with proving that the transactions are fraudulent -- which can be a time-consuming process.

While the cashers were draining bank accounts, U.S. Bank, one of the financial institutions hit by King, was telling reporters that no customers lost money.¹⁶

Thomas doesn't know how much the King operation brought in altogether because King had other cashers working other banks for him in the United States and Europe, such as a 24-year-old Texan named Douglas Cade Havard, who authorities said absconded with millions before being arrested with a partner in the United Kingdom in 2004. British officials said that Havard and a 25-year-old Scot named Lee Elwood stole about \$11.4 million over 18 months. They were caught only after an accomplice was arrested in Austin, Texas, trying to board a plane carrying \$30,000 in \$20 bills.¹⁷

As for King's operation with Thomas, the Russian was so happy with the success of the U.S. Bank phish that Thomas authored for him, that he decided to phish the Federal Trade Commission as well. He said he hated President Bush and wanted to attack a government financial institution. Thomas explained that it wasn't the FTC he wanted, but the Federal Deposit Insurance Corporation. The phish, which Thomas helped write, went to 40 million addresses in 24 hours, according to Thomas.

The mail told recipients that the FDIC had suspended federal deposit insurance on their bank account due to suspicious activity that violated the Patriot Act. The consumer could lift the ban at the FDIC's IDVerify page (a bogus site hosted on a server in Pakistan) by providing their debit card and PIN number for verification. Failure to comply could result in a visit from the Department of Homeland Security.

But, tipped off to the phishing attack, the FDIC issued a special public alert about the scam, and few people fell for it. The agency also phoned the Pakistani hosting company and persuaded it to take down the fake site.¹⁸

Things grew more harried with the King Arthur schemes, when money that the U.S. Bank cashers wired to Russia suddenly stopped going through. Thomas says the FBI allowed about \$17,000 to find its way to Eastern Europe before blocking the rest.¹⁹

King wasn't pleased. He'd left Shadowcrew after proceeds from cashing operations based there stopped flowing to him. Now the same thing was happening at TheGrifters. He wanted the cashers to return to Western Union and recover the blocked funds, which in some cases meant sending cashers back to cities they'd left. "It was a ... nightmare," says Thomas. "You knew there (wasn't) going to be any recovery ... because the feds had locked that money up."

Then Myth started ripping. In Oregon, he had 100 bank accounts to cash out one day, but claimed most of them didn't work.²⁰ Things were getting out of hand. As King pressed Thomas to come through with the missing Western Union cash, one of Thomas' enemies at Shadowcrew discovered that King was doing business with Thomas and sent a copy of his old Issaquah police report to the Russian.

Butler had had enough.

"(Butler) calls me up and says, 'Shut it down, we're not doing it anymore,'" Thomas says. And that was the end of the King operation. It wouldn't be long before it was the end of TheGrifters, CarderPlanet and Shadowcrew, too.

It was mid-March 2004, and David Thomas was chatting online with a young hacker who went by the nickname "Ethics," when the latter suddenly asked him: "btw, you know anyone who would pay to get celebs private cell phone numbers? or any other number's from t-mobile's database?"

Thomas replied, "hehehehehe oh man that would be so fuking cool."

Ethics, aka Nicolas Jacobsen, did little on the boards but talk, Thomas says. He once discussed building a miniature submarine with carder middleman "Myth" to run cocaine from Colombia. But mostly he procrastinated and disappeared when it came time to do any jobs. So when Ethics told Thomas he'd hacked a T-Mobile server and had access to billing information and passwords for the company's 14 million customers, Thomas was skeptical. That is, until Jacobsen sent him Paris Hilton's Social Security number and password, as well as the security question and answer to her T-Mobile account and photos from her camera phone.

Thomas didn't know it, but Ethics also had the password for the T-Mobile account of a Secret Service special agent named Peter Cavicchia who worked in the agency's cybercrime division. Sifting through the agent's e-mail, Ethics found documents related to a Secret Service sting operation, including, incredibly enough, evidence that the Secret Service was monitoring Ethics' own ICQ chats.

Ethics had stumbled into the most organized and ambitious operation against online scammers in U.S. history. While Thomas had been working on the West Coast for the FBI, the Secret Service's New Jersey office had infiltrated Shadowcrew separately, with the help of a confidential informant, and begun gathering evidence against carders on that site. The sting known as "Operation Firewall" began when police arrested a top administrator of the Shadowcrew site in the summer of 2003 and called in the Secret Service.

Secret Service agent Larry Johnson says his agency didn't initially realize the value of their catch. Once they did, they quickly flipped the suspect and sent him back to Shadowcrew to avoid suspicion that he'd been arrested.

With the informant's help, they set up a private, encrypted computer network where Shadowcrew members could, ostensibly, communicate in secret. In reality, the network was run from the Secret Service's office in New Jersey, where communications were recorded and IP addresses tracked.

The Secret Service won't discuss the identity of its informant, but today Thomas and other carders believe it was a scammer known as "Cumbajohnny," or "CJ", who appeared on Shadowcrew in the summer of 2003. When Shadowcrew's Kim "Macgyver" Taylor was jailed in Colorado around that time, CJ assumed control of the site.

Though Thomas wasn't privy to the Secret Service operation, he suspected early that CJ had flipped. It was CJ, he says, who, in February 2004, invited Shadowcrew members to join the VPN that turned out to be under surveillance. Thomas says CJ also tried to sell members \$150 AT&T calling cards that would allow them to make \$1,000 to \$7,000 in calls. Thomas thinks the cards were set up to allow authorities to trace the callers.

Thomas became more suspicious of CJ when, in March 2004, Dmitry Golubov, aka "Script," disappeared from CarderPlanet, and CJ assumed a role on that board, too. It was CJ who had sent "King Arthur" Thomas' arrest report discussing federal agents and the Russians in an attempt to sabotage his dealings with King. Thomas sent CJ a note taunting him with his own accusations. "hey cumbacop ... so you're running (CarderPlanet) now eh ... did you bust script? ... so I guess your shiny badge is real shiny now."²¹

It was 1 a.m. and the message was barely gone before Thomas' handler, Seattle FBI Agent Steve Butler, called him. "What are you doing? Who were you just talking to?" Butler demanded to know. When Thomas mentioned Cumbajohnny, the FBI agent grew angry. "These guys over there can shut you down in an instant," Butler said. "Don't you ever talk to him again."

"I knew right then that Cumbajohnny wasn't kosher," Thomas says.

The ongoing turf battles between TheGrifters and Shadowcrew administrators highlight a problem inherent in law enforcement agencies employing criminals in their operations. Such operatives come to the task bearing grudges and ego issues that can easily derail an investigation if not carefully managed. If Cumbajohnny was the Secret Service's informant, it meant that agents for the FBI and Secret Service were essentially battling to blow each other's covers.

Regardless of Butler's warning to stay away from CJ, Thomas continued to taunt the carder and other members online. His enemies stepped up their attacks against him as well, tracing him to Seattle and attempting to locate his apartment to post pictures of it on the board. For the first time, Thomas began to fear for his safety.

Then things started to change.

Butler had been warning Thomas to stay away from CarderPlanet -- implying that events were about to converge on the Russian carding site.

In July, Douglas Havard was arrested in the United Kingdom; shortly afterward, CarderPlanet suddenly shut down. King Arthur had taken control of the board by then, and, according to authorities, he and other senior members of the site decided it was time to take their operation deeper underground to make it harder for police to track them.

In a note explaining the decision, King wrote: "This forum made them (LE) smarter and kept them in the loop of happening.... Now, everything will be the same, but (they) will not know where the wind is blowing from or what to do."

In September, Butler announced he was leaving the cybercrimes task force for a new assignment with the Joint Terrorism Task Force and abruptly pulled the plug on TheGrifters.²² Thomas says he was caught off-guard. "I thought it was going to be a long-term job that would last for five to 10 years," he says.

The other shoe dropped at 9 p.m. EST Oct. 26, 2004, when police and federal agents swooped in on more than a dozen Shadowcrew members in several states and Canada in a coordinated bust. The Shadowcrew admins had told the members to convene online at the appointed hour for a mandatory discussion, ensuring they'd all be caught at their computers at the same time.

Authorities nabbed 19 people in the bust, among them Kim Taylor, Thomas' former partner, who'd been released from jail a few months earlier. Ethics was nabbed separately. Cumbajohnny was the only major Shadowcrew admin whose nick did not appear on the indictment.

Taylor pleaded guilty to one count of access-device fraud (another charge was dropped) and was sentenced to 30 months in jail and three years' probation. He's scheduled to be released from federal prison at the end of March.

His lawyer, Bruce Rosen, says, "He did something, and he deserved to go to jail," but that the charges against his client were exaggerated. Taylor maintains he was only a forum moderator on Shadowcrew, not an administrator as authorities made him out to be, and that the title was in name only -- he never engaged in an active role as a moderator.

The Shadowcrew bust was touted as a major success by law enforcement. Since the initial action, subsequent arrests in Operation Firewall have brought the total number of carders nabbed to 38 globally. Authorities say the suspects trafficked in more than 1.5 million stolen credit card numbers, resulting in losses estimated to be at least \$4 million. The sting also netted more than 8.5 terabytes of forensic evidence -- the equivalent of 2.2 billion pieces of paper -- and involved more than a dozen criminal task forces in the United States and elsewhere.

But the long-term effects of the operation on curbing criminal activity have proven to be almost nil. It wasn't long after Shadowcrew went down before new carding sites, such as CardersMarket and the International Association for the Advancement of Criminal Activity, or IAACA, popped up to take its place. And the bust opened the way for new problems as well.

Amir Orad, executive vice president of security company Cyota (now owned by RSA Security), which has a command center in Israel from where researchers monitor the carding boards, says Operation Firewall made it more difficult for law enforcement to track carders. Once Shadowcrew went down, the community morphed from a small number of large carding sites to a larger number of small sites that have become harder to trace and infiltrate. And many of the most serious criminals have disappeared from the boards altogether, taking their activities further underground.

"What we see clearly is that taking down ... one group doesn't solve the problem, it creates multiple small problems," Orad says. "(We) haven't seen a major impact of those arrests besides maybe the publicity and the awareness that this whole crime costs."

Others have also disputed law enforcement's characterization of the significance of Shadowcrew's role in cybercrime, saying the website was more a sandbox for kiddie criminals than a virtual Cosa Nostra, and that those who were arrested were mostly low-hanging fruit.

Attorney Rosen said in a statement to the New Jersey court that although his client Taylor acknowledged that many of the activities on Shadowcrew were illegal or nefarious, the site was really just "a highly unorganized, inefficient message board frequented by immature geeks and social misfits."

It's two years since Thomas says the FBI ended his work with them, and he and I are walking on a Midwest college campus where he now lives in student housing. After the FBI dropped him, he enrolled in the college's journalism program to keep from returning to a life of crime and to write his life story. As we stroll the campus pathways, clear-eyed students pass by, their futures still in front of them.

"I want their lives," Thomas says with the envy of someone who's halfway through his life and knows that his options are running out.

The campus is surrounded by snow-capped mountains, but the fresh air and scenery are lost on a digital animal like Thomas, who rarely leaves his apartment. Though he no longer works for the FBI he still wakes early before classes to jump on the boards and see what's happening and stays online after school until late in the evening. The draw of the boards, when he has little to take their place, is too strong.

He's more than a little bitter about the way the FBI dropped him. After Butler pulled the plug on TheGrifters, Thomas says they discussed building a similar site to attract



terrorists for the Joint Terrorism Task Force. But after Thomas developed a site, Butler failed to get approval for the project and cut Thomas loose.

For a time, Thomas kept TheGrifters online and turned it into an "anti-carding site" with a few associates, including "John Dillinger." They spent hours building dossiers on carders and tracking arrests, and amassed a large database of information, including part of the Shadowcrew database that someone copied after the bust. Thomas hoped to turn it into a resource for law enforcement and use it as a platform to warn kids away from crime, but it hasn't worked out that way.

"Crime is often harder work than a regular job," he says. "Every time I've done something -- it doesn't matter what it is, counterfeiting or whatever -- it's always been more work than a regular job would have been. And I would have much rather had a real job than be involved in a criminal act because it's less ... stress."

Of his associates from TheGrifters, only Dillinger knows about his work for the FBI. Thomas wanted to tell the others, he says, but some of them defended him when his enemies accused him of working for the feds, and it's hard for him to explain to them why he did what he did. He realizes that this article will likely make him a pariah in the community.

"The people on the fringes of society are the only ones who ever accepted me," he says. "Now I feel I've destroyed that for what I did for the government." Thomas' job with the government also cost him his relationship with Bridget Trevino, who left him about four months before the work ended because of his obsession with the boards.

"I became so unhappy because I never got to spend any time with him anymore," she says. "Even though we were in the same room together, I was alone."

Thomas says the FBI has threatened him with imprisonment in Texas, where he has an outstanding warrant for check fraud, if he talks to the press about what he did for them. "They don't want me discussing what the government was allowing to happen. They don't like the fact that people were authorized to do major crimes like that," he says²³.

There's a touch of self-destruction to his decision to talk now. He wants to leave the boards behind but lacks the willpower to do so. He knows that once this story is public, he'll have to close the chapter on "El Mariachi" and just be David Thomas again. "And maybe that's what I want," he says. "I want to get on with my life."

For years he's had no offline friends and now is having to get used to being around other people again. Last spring, when the winter thaw was gone and people at his college were starting to emerge outdoors again, he walked the campus green looking at students and teachers lounging on the grass in the sun and thought to himself, "God, this is just so beautiful."

"I feel like I've been locked up for years and years and years and I've just gotten parole," he says.

But that's only during the day. At night, he's back in a dark room, surfing the boards.

Ø

Wired.com © 2007 CondéNet Inc. All rights reserved.

FOOTNOTES:

¹... posts from his former website, The Grifters. The logs appear to be legitimate but Wired News was unable to verify that they were recorded on behalf of the FBI or that they were unaltered by Thomas.

² Campbell asked Wired News not to publish his real name for fear that other thieves would target him.

³ ... and lists of possible relatives. According to Thomas, Decep had previously worked for a Florida prosecutor and had access to a Lexis-Nexis database used by law enforcement agents and businesses.

⁴ ... trying to withdraw money from Fortis. I was unable to confirm the arrest in Brussels with either Schwab or the FBI.

⁵ "If we had left it up to Schwab, they might never have gotten the FBI involved at all." Even then, it was the Oregon sheriff's department that nailed the suspect on unrelated charges. And the Oregon prosecutor handling the identity theft cast against the suspect says no one told him about the Schwab crime and investigation. The victim, Campbell, said he was told that authorities were able to connect the suspect to the theft of his Schwab money because the suspect had changed the contact phone number on his account to the suspect's real cell phone number. I was unable to confirm this.

⁶ "They told me that they'd take care of me, and I'd have a legit job with them." One of Thomas' former public defenders in Seattle, Thomas Hillier, was reluctant to speak with me but confirmed the jailhouse visit with Butler. He said his memory of the fouryear-old case was foggy and that he didn't recall a federal job offer for Thomas, although his file notes do contain a cryptic reference to a job offer next to the name of former assistant U.S. Attorney Hugh Berry. According to Thomas, Berry was the U.S. attorney who visited him in Nebraska with FBI agent Steve Butler.

The Nebraska prosecutor, Andrea Belgau, who Thomas says was present at the Nebraska meeting with Butler and Berry, was also very reluctant to discuss the meeting. "I can't speak very completely about it other than he did offer assistance to the federal authorities," she said. She wouldn't discuss the details, but said she wouldn't dispute what Thomas told me either. "I don't think it's appropriate for me to delve into it," she said. "The defendant may be free to speak about it, but those of us employed by government agencies have more restrictions."

⁷ "It was a win-win situation." Thomas says the FBI paid him no salary, but covered his rent and expenses. The former apartment manager at the complex where Thomas lived confirmed that the FBI paid rent on the apartment and that FBI Agent Steve Butler and another agent whom the manager identified as an FBI district supervisor accompanied Thomas the day he and Trevino moved in. The manager, who asked not be identified by name because he spoke without permission from his former employer, said Butler gave him his cell phone number and told him to call if Thomas caused any problems while living there.

Candace Hamel, who worked in the property management head office at the time, said she couldn't confirm that the FBI paid for the apartment, but then added after a pause and without prompting, "I'm not denying it either." When asked if the management company had an ongoing deal with the FBI to supply the agency with apartments, as Thomas contends, Hamel again said she couldn't confirm or deny then added, "That's confidential information."

FBI Agent Steve Butler was polite and friendly but declined to comment on whether Thomas worked for the FBI. "We would never confirm or deny something like this," he said, saying that such comments would make other people reluctant to work in such capacity with the FBI. I should note here that there is a David A. Thomas who works for the FBI as chief of the agency's Cyber Division Criminal Computer Intrusion Unit. He's often quoted in articles about cyber crime and should not be confused with David R. Thomas, who is the source for this story.

- 23 -

WIRED NEWS

⁸ Butler would make sure that he went to prison, and that other inmates would know he'd worked for the FBI Thomas says he was cowed by Butler's threat and never considered committing crimes behind his back because he assumed the feds were watching his every move. But recent court records involving another carder in South Carolina show how easily a criminal working for the feds can commit crimes under the nose of agents who are supposed to be watching him. According to an affidavit in the case, while working a few hours each day out of a government-supplied apartment, this other carder allegedly continued to card secretly on the side.

⁹"If he had \$50 left on the card, he'd go find another item to max out the card," Thomas says. Some sources say Big Buyer was arrested in 2003 in Russia, but I was unable to confirm this.

¹⁰ ... and the party's bank say they never received the wire transfer request. Tattrie initially said he didn't know anything about the issue, then in a follow-up call months later acknowledged that authorities had contacted him about it. But when I tried to confirm with Tattrie the authenticity of an Excel spreadsheet that BoBaBc supposedly took from his computer, Tattrie told me to send it to his lawyer, then wouldn't give me his lawyer's name or contact info. Without BoBaBc's real name, I was unable to verify that an investigation existed. Local and federal law enforcement agents in Kentucky and Arizona said they had no knowledge of a case involving Tattrie's hacked computer and the Democratic Party or anyone who went by the BoBaBc nick. As for the fax, bank officials said the scheme would never have succeeded -- in part because some key information on the fax was incorrect.

¹¹"Mesh" and "Nasa" decided to phish the Ralph Nader campaign site. Calls to the party offices to confirm the phishing attacks were not returned.

¹²... that would authenticate debit and credit cards to an ATM. At the time, banks used a special number, or algorithm, to authenticate their cards. If a thief tried to encode an account number onto a blank card without the algorithm, the card wouldn't work in an ATM machine. By entering a card's number in the algorithm generator program, they could determine the algorithm used by that bank. Not all of the programs were successful, however. King's generator was known to be one of the best. The banks later caught on to what the carders were doing and changed their methods for authenticating cards.

¹³ ... earlier this year before he was arrested. Dillinger, who recently signed a plea agreement with authorities, is awaiting sentencing in Virginia. It's unclear from court documents and from law enforcement statements whether the crimes he's charged with stem from crimes he conducted during the King operation, or whether the charges relate solely to other crimes he committed with different conspirators.

¹⁴ **Decep claimed to pull \$11,600 from nine cards one night. Myth got \$90,000 in a few days, according to Thomas** When a similar wave of ATM cashing occurred in March 2006, a banking-security analyst with Gartner was widely quoted in news articles saying this was a new kind of attack using PIN numbers stolen from a database. Thomas' account of the King operation makes it clear that these kinds of debit card and PIN attacks have been going on at least since late 2003, but received little attention. This is either because banks managed to keep them quiet or because these kinds of attacks weren't on the media radar until a database belonging to CardSystems Solutions, a company that processed credit card payments, was hacked in 2005, exposing 40 million debit and credit card numbers.

¹⁵ ... and kept copies of ATM receipts, which the cashers were required to scan. I called the Florida woman whom Thomas identified as Decepgal, but she wouldn't comment on her role in the cashing operation. "I really don't like talking about that," she said and declined to say any more. We're not publishing her real name because she has not been charged with the crimes discussed in this article.

¹⁶... U.S. Bank, one of the financial institutions hit by King, was telling reporters that no customers lost money. U.S. Bank spokesman Steve Dale said he was unaware that the phishing scam occurred, although an article from the time quotes him discussing it. He said he doubted the FBI would allow cashing operations to occur. But when pressed to check with his company's fraud investigators to determine if U.S. Bank had cooperated with the FBI to allow the cashing to occur in order to observe the criminals in action, he called back to say, "We're not going to substantiate, confirm or deny anything. We would not want to be in a position where we interfere with any kind of investigation."

¹⁷ ... trying to board a plane carrying \$30,000 in \$20 bills. The FDIC phish is archived at the website for the Anti-Phishing Working Group. According to Thomas, the FBI tipped off the FDIC to the scam. FDIC spokesman David Barr confirmed that FDIC lawyers contacted the Pakistani host, CubeXS, and that the site was taken down the same day it went up. He said, however, that his agency learned about the phishing attack not from the FBI but from someone who had received a copy of the phishing e-mail. I asked him to double-check with his agency's fraud department to see if the FBI hadn't warned them of the attack but he never called back with a response or answered follow-up calls. U.S. Postal Inspector Greg Crabb told Wired News, without prompting, that Thomas had helped King Arthur author phishing attacks against the FDIC and banks. When asked if he was aware that Thomas was running TheGrifters for the FBI, he said yes.

¹⁸ **The agency also phoned the Pakistani hosting company and persuaded it to take down the fake site.** The FBI wouldn't comment on anything related to the information that Thomas provided me. I supplied Western Union spokeswoman Kristin Kelly with specific transaction numbers to verify that the transfers went to the recipients and Eastern European destinations that Thomas indicated, but she wouldn't comment on specific transactions or say whether any of the money transfers had been blocked. She did say



- 24 -

that Western Union collaborates with law enforcement requests to investigate unlawful activity and does sometimes block transactions it suspects are suspicious.

¹⁹ **before blocking the rest.** Law enforcement agents from two agencies told me they'd heard that Myth was arrested in Seattle in 2004, but no one has been able to provide a real name or specifics about the arrest. Several attempts to verify the arrest through official channels have been unsuccessful.

²⁰ In Oregon, he had 100 bank accounts to cash out one day, but claimed most of them didn't work. According to U.S. Postal Inspector Greg Crabb, Havard was working with King Arthur and his roommate in Russia, who went by the nick "Diesel." The two Russians provided Havard and his cashing partners with card and PIN numbers for Citibank and other financial institutions.

²¹ "... so I guess your shiny badge is real shiny now." For reading clarity, Wired News has corrected some spelling errors in quotes taken from chat logs.

²² Butler announced he was leaving the cybercrimes task force for a new assignment with the Joint Terrorism Task Force, and **abruptly pulled the plug on TheGrifters.** An FBI spokeswoman confirmed that Butler has moved on from the Northwest Cyber Crimes Task Force but would not discuss his new assignment.

²³ "They don't like the fact that people were authorized to do major crimes like that," he says. Thomas says during the time he worked for the FBI, Butler promised he'd put in a good word for him in Texas to help get the old warrant removed from his record. That never happened, and as this article was being edited, Thomas was indicted and jailed briefly on the decade-old Texas warrant. The timing of his arrest likely had less to do with him speaking to the press, however, than with him angering authorities with what he'd been saying on the boards at the time. Thomas is currently trying to negotiate the Texas charge down to a fine. Additionally, he filed a Freedom of Information Act request, with help from the American Civil Liberties Union, to try to obtain records related to his work for the FBI but received an ambiguous response stating that the records might be classified while at the same time denying that any records exist.