STAYSAFEONLINE.org
National Cyber Security Alliance
symantec
USA TODAY Education
AS SEEN IN USA TODAY'S NEWS SECTION, JULY 11, 2005

Cybercrooks lure citizens into international crime

By Keith Simmons, USA TODAY

Cyberthieves are turning ordinary people into 'mules,' or unwitting collaborators, who reship goods bought with stolen identities

By Byron Acohido And Jon Swartz
USA TODAY

GRASS VALLEY, Calif. — To Karl, a 38-year-old former cab driver aspiring to a career in real estate sales, the help-wanted ad in the newspaper radiated hope.

The ad sought "correspondence managers" willing to receive parcels at home, then reship them overseas. The pay: $24 a package.

Karl applied at kflogistics.biz, a fraudulent website imitating a legitimate site. He quickly received an e-mail notifying him that he landed the job, followed by e-mail instructions on how to take receipt of digital cameras and laptop computers, affix new shipping labels and "reship" them overseas. Easy enough.

Within weeks, he had sent off six packages, including cameras and computer parts, to addresses in Russia. Little did Karl know that he had become another unwitting recruit in a growing scheme to aid online criminals, the latest wrinkle in frauds that cost businesses hundreds of millions of dollars a year.

Before long, Karl began to feel like Sydney Bristow from TV's Alias, who wrangles her way through the Eastern European underworld.

Fearing retaliation, Karl asked that his real name not be used.

One day, a $4,358 electronic deposit appeared in Karl's online bank account, followed by e-mail instructions to keep a small amount as his pay and wire most of it to Moscow.

Then Karl began receiving account statements intended for online banking customers from around the USA. Someone had changed the billing addresses for stolen credit cards and bank account numbers to his residence in Grass Valley.

One of the letters was intended for 28-year-old Ryan Sesker of Des Moines, Iowa, letting him know his credit limit had been raised to $5,000 — a request he never made. Around the same time, a USA TODAY investigation found, someone accessed Sesker's online banking account and extracted $4,300.

"I thought I could work a few hours a day and make a couple hundred bucks, not get sucked into something out of Alias," says Karl, sipping steamed milk in a cafe.

What he became, in fact, was a "mule."

Karl and other ordinary citizens are being

Cybercrime Inc.'s pipeline

As more people use the Internet to shop and bank online, crime groups have stepped up Internet-enabled thefts. Much of the activity revolves around using stolen personal and financial data to carry out elaborate schemes to channel goods and cash out of the USA. Mules — unwitting citizens looking to legitimately earn extra cash — play a key role moving goods and insulating the criminals from detection.

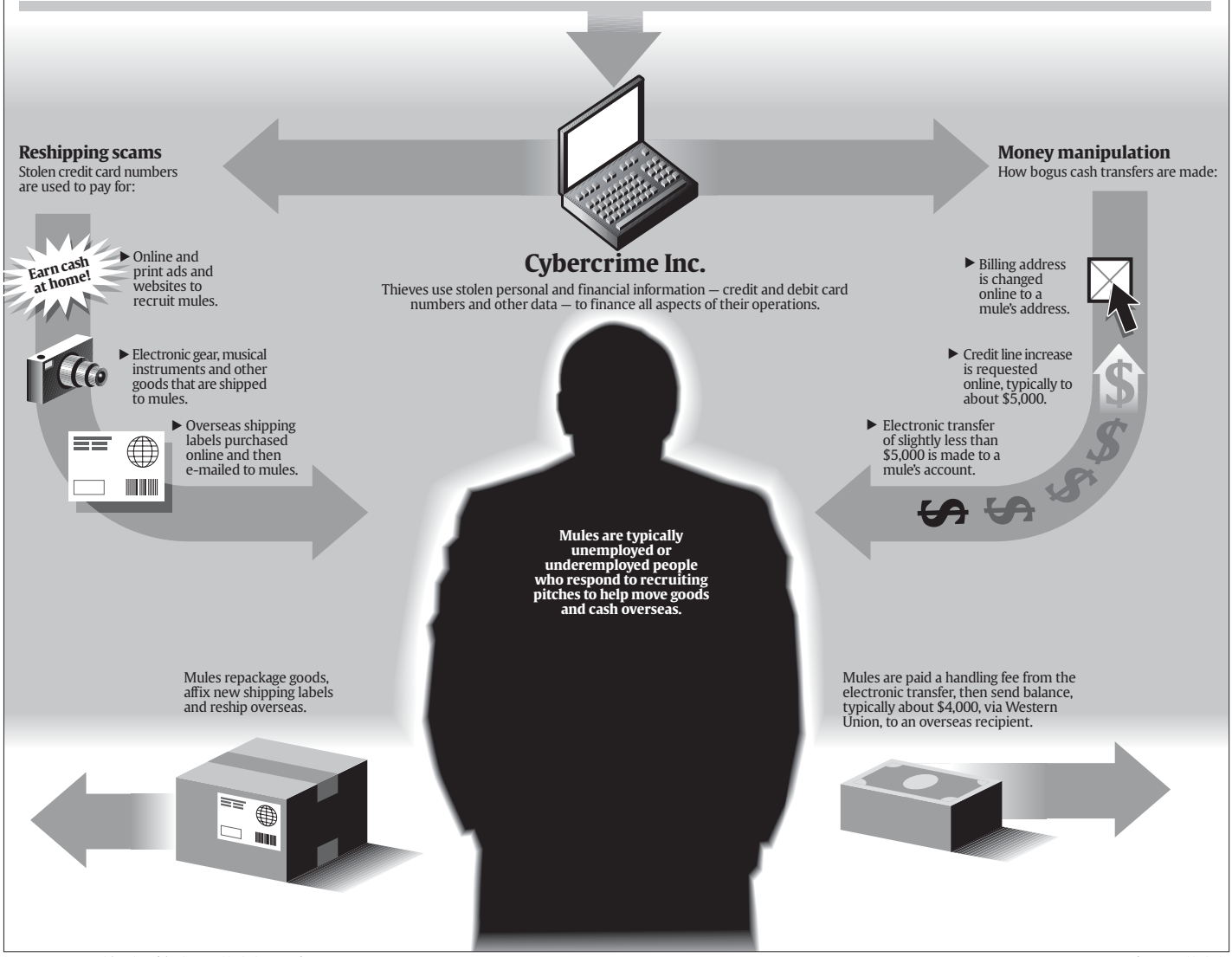
Pool of lost and stolen IDs
Personal and financial data on 50 million individuals have been lost or stolen this year.

▶ Lost backup tapes
Citigroup, 3.9 million customers; Bank of America, 1.2 million federal employees; Time Warner, 600,000 employees.

▶ Database breaches
CardSystems, 40 million credit card account records; DSW Shoe Warehouse, 1.4 million customer records.

▶ Insider thievery
675,000 branch customers from Bank of America, Wachovia, PNC Bank of Pittsburgh, Commerce Bank of New Jersey; Georgia DMV, 200,000

▶ Phishing attacks
E-mail scams add potentially millions more stolen IDs to the pool.



Sources: FBI, Internet Crime Complaint Center, USA TODAY research

By Frank Pompa, USA TODAY

widely recruited by international crime groups to serve as unwitting collaborators — referred to as mules — in Internet scams that convert stolen personal and financial data into tangible goods and cash. Cybercriminals order merchandise online with stolen credit cards and ship the goods overseas — before either the credit card owner or merchant catch on. The goods then are typically sold on the black market.

Mules serve two main functions: They help keep goods flowing through a tightly run distribution system, and they insulate their employers from police detection.

To document what such a mule goes through, USA TODAY spent five months pursuing leads from law enforcement officials, tech security experts and Internet underground operatives. The probe uncovered fresh evidence detailing how organized crime groups, such as the one that enlisted Karl, operate quietly at the far end of the cybercrime pipeline.

Savvy thieves often keep rip-offs below $5,000 to avoid detection from bank monitors and the FBI — but cumulatively, the thefts reach into hundreds of millions of dollars.

While e-mail phishers, hackers and insider thieves grab

notoriety for stealing personal and financial data, these reshipping groups put the stolen IDs to use. Security consultant eFunds estimates that reshipping rings set up nearly 44,000 post office boxes and residential addresses in the USA as package-handling points in 2004, up from 5,000 in 2003. And they show no signs of slowing.

The dark side of e-commerce

Consumer-level financial fraud has been around since thieves first thought to filch blank checks from mailboxes. The Internet has taken it to a new level, not yet fully understood by the general public.

No one really knows how much of the estimated $150 billion worth of online transactions this year will be fraudulent, but e-merchant losses pegged to reshipping scams were estimated at $700 million in 2004, up from $500 million in 2003, according to eFunds.

Cybercrime has morphed into two broad areas:

▶ Hackers, insider thieves and phishing con artists focus on pilfering personal and financial data, such as names, addresses, birth dates, mothers' maiden names, driver's license numbers, credit card numbers, Social Security numbers, passwords and personal identification numbers, or PINs.

▶ The ID thieves, in turn, supply crime organizations that use the stolen data to fleece online merchants and banks with the help of unwitting mules.

"Any of these job postings that get consumers to receive and forward packages and/or money are bogus," says Barry Mew, a U.S. postal inspector in California.

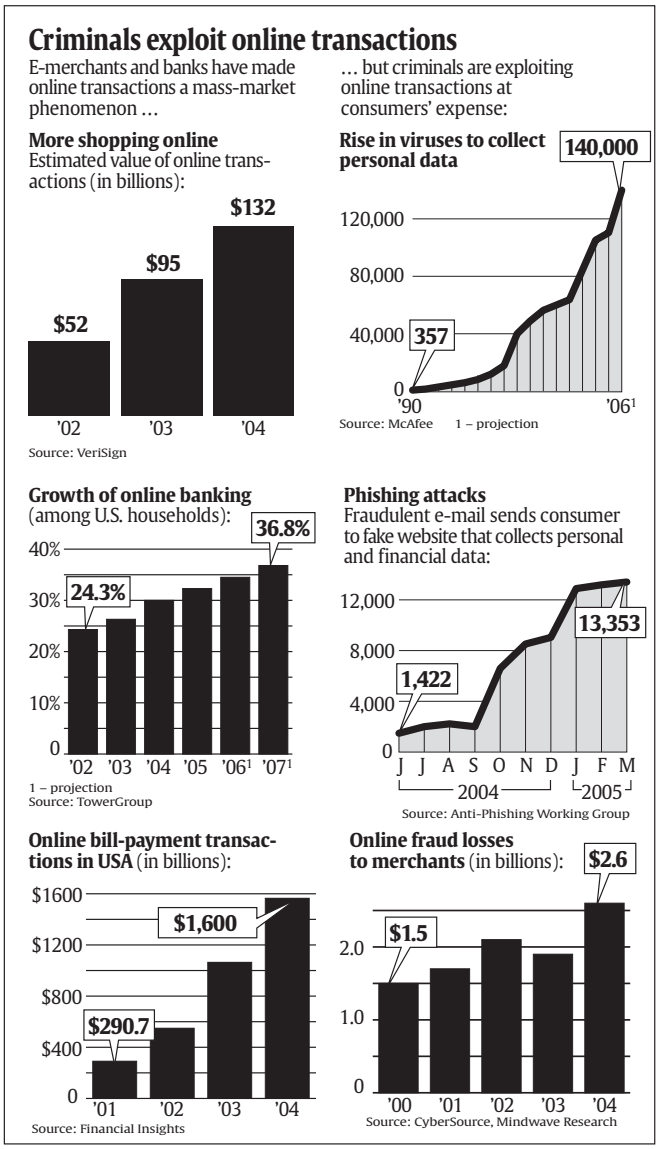
Consumers who report false charges typically are reimbursed by the banks. But some are drawn into messy identity-theft scams. Law enforcement can't keep up, for a variety of reasons. The FBI has led sting operations to knock out reshipping gangs in Romania and Nigeria. But cabals such as the one that recruited Karl thrive in Eastern Europe, Brazil and, most recently, the Philippines.

With e-commerce at record levels, the risk of you or someone you know getting defrauded is rising. "The fear is if we don't get on top of this and protect the consumer better, we'll see more account skimming and deeper kinds of identity thefts happen," says George Tubin, senior analyst at banking consultant TowerGroup.

Luring recruits

The 16-line classified advertisement that appeared April5 in The Union in Grass Valley beckoned like a life preserver: "Look at this! WORK at Home! Correspondence manager vacancies. MAIL PACKAGES from home without leaving your current job. Easy! Ship parcels from our clients. Get Paid $24 per parcel! Info: http://kflogistics.biz/vacancies.asp.htm."

To Karl, the prospect of getting paid to reship packages in his spare time seemed like a godsend. He had dabbled in online marketing and was studying to get his real estate license. Something like this could tide him over.



By Adrienne Lewis, USA TODAY

Union records show the ad was ordered and paid for online, using a credit card with a Milford, Mich., billing address. Chauna Renaud, The Union's classified ads manager, says no one from The Union spoke to the buyer, who paid $427.97, and that no theft victim has sought to refute the transaction.

Detective Bill Netherby of the Nevada County Sheriff's Office says the ad almost certainly was paid for with a stolen credit card.

Companies such as kflogistics.biz put a new twist to an old ruse.

Merchants have long become wary of shipping expensive goods overseas. But thieves know that once an online transaction is approved, shipments inside the USA receive scant scrutiny, especially during high-traffic holidays, says Julie Fergerson, vice president of eFunds and co-chair of the Merchant Risk Council, an industry group formed to fight

online fraud.

So they've taken to recruiting U.S.-based reshipping mules whose homes function as drop points.

There likely are dozens of reshipping operations in existence, though no one has precise figures. In its investigation, USA TODAY — with the help of law enforcement officials, postal inspectors and computer security experts — identified 21, most with polished websites and slick online job-applications.

USA TODAY's investigation also found that reshipping groups recruit mules on popular employment websites, such as Monster.com and CareerBuilder.com, order goods from e-merchants large and small, and even pay for shipping charges via online services designed to streamline credit card transactions. FBI Supervisory Special Agent Dale Miskell, a cybercrime specialist, and other fraud inspectors confirmed USA TODAY's findings.

A reshipping group going by the name U.S. Mail Service last February, for instance, used a credit card to pay $97 for a three-month ad on Jobfinder.com. Jobfinder CEO David Lizmi could not confirm that a stolen card number was used. But fraud inspectors say reshipping groups routinely pay for ads with stolen account numbers. Lizmi says he pulled the ad after receiving a complaint. U.S. Mail Service never contacted him for a refund, and no one has stepped forward to dispute the payment.

Monster.com and CareerBuilder.com say they deploy teams to screen ad orders, investigate complaints and educate customers about scams. But reshippers skirt such defenses by changing names and websites every few months. "They are so good at sneaking things through," says Michele Pearl, vice president of compliance and anti-fraud at Monster.com.

Mule recruiters typically direct job applicants to well-crafted, company websites. "Registering a domain name and putting up a website to perpetrate these schemes is easy and cheap," says Joe Stewart, analyst at Lurhq, which provides computer security for businesses.

The name kflogistics.biz imitates an existing website, kflogistics.com, registered by a legitimate El Paso freight-forwarding company. The copycat website lists someone calling himself Michael Birman as the registrant, with a New York mailing address and phone number. The last two letters of Birman's listed e-mail address, tyler052@yandex.ru, indicate kflogistics.biz has a Russian base.

Attempts to contact Birman and kflogistics.biz were unsuccessful. Most website registration data are "almost certainly bogus," says Stewart.

Hungry job applicants

Recruiters are being drawn to a U.S. job market teeming with unemployed and underemployed able-bodied citizens hungry to earn extra income, says Paul Krenn, a spokesman for the United States Postal Inspection Service.

"Most of them don't ask questions," Krenn says.

Irene Rodriquez, 38, a longtime bulk-mail handler from San Jose, Calif., regularly surfed employment websites, such as Monster.com and CareerBuilder.com, partly owned by Gannett, USA TODAY's parent, looking for opportunities to earn extra income. Hoping to pay for her daughter's senior prom gown, Rodriquez last February responded to a U.S. Mail Service pitch she spotted on Jobfinder.com. U.S. Mail offered $30 to $50 per reshipped package.

"When you see a job listed on a respected website, you think it's legitimate," says Rodriguez. "I thought this was a legal company."

About the same time, Lynn Malito, 46, a single mother of two, got laid off from her job as a dispatcher for a trucking company in Memphis. Malito says she responded to an online ad on Monster.com to handle reshipping chores for CNetExpress — whose name mirrors online media company CNet. She also considered a similar job offer she found on Monster.com from something called TSR Corp.

Karl, Rodriquez and Malito all ended up working as reshipping mules but cut off their activities and reported their experiences to authorities after becoming suspicious about the work. "It petrified me," says Malito.

Only the most egregious mules run the risk of going to jail. As a former federal cybercrimes prosecutor, Paul Luehr let go a number of mules he had tracked down, "because we could uncover little or no evidence of their criminal intent." Luehr, now general counsel at tech consultant Stroz Friedberg, says the naive reshippers "thought they had a regular job."

Often the easy tracking ends at the mule's U.S. residence. Once the item or cash moves overseas, diplomatic protocols and differing cultural priorities can quickly turn the trail cold, says Luehr.

Recent security lapses

Personal data for nearly 50 million people have been stolen or lost this year:

	Name	Type of breach	Individuals affected
Feb. 15	ChoicePoint	System hacked	145,000
Feb. 25	Bank of America	Backup tapes lost	1.2 million
April 1	Georgia DMV	Insider theft	200,000
April 8	San Jose Medical Group	Stolen computer	185,000
April 12	LexisNexis	Passwords compromised	312,000
April 14	Polo Ralph Lauren	System hacked	180,000
April 18	DSW Retail	System hacked	1.4 million
April 20	Ameritrade	Backup tapes lost	200,000
April 28	Wachovia, Bank of America, PNC Financial Services, Commerce Bancorp	Insider theft	675,000
May 2	Time Warner	Backup tapes lost	600,000
June 6	CitiFinancial	Backup tapes lost	3.9 million
June 16	CardSystems	System hacked	40 million

Source: Privacy Rights Clearinghouse

By Adrienne Lewis, USA TODAY

U.S. and foreign authorities have arrested reshipping group leaders in Nigeria, Ghana and Romania. But those were comparatively small-scale operations. "It's like a high-end fencing operation," says John Pironti, a security consultant at Unisys who specializes in bank systems. "The idea is to move this stuff overseas and remove traceability even further."

Goods on the move

Over a three-week period in April, Karl, who cooperated with police and won't be prosecuted, reshipped half a dozen parcels for kflogistics.biz. He followed e-mail instructions from someone who identified himself as Michael Birman, the same name listed as the website's domain registrant.

Occasionally, Karl spoke by phone with Birman, who once boasted to Karl that he managed a network of 200 people.

Karl might have continued as a reshipper had Birman paid him $24 a parcel as promised. Instead, Birman tried to manipulate Karl into deeper activities. Things began to unravel in early May once Karl began to press Birman for a paycheck.

Birman responded by asking Karl if he had an online account at Chase Bank, Citibank or Washington Mutual into which kflogistics.biz could deposit his pay. Fraud inspectors say this indicates Birman already had fraudulent access to a portfolio of online accounts in those banks and was maneuvering to sweep Karl's account into the mix.

Karl balked at first, but after discussing the matter with his bank manager, he gave Birman the routing and account numbers for his checking account at the Nevada City branch of Bank of America. The bank manager, Paul Shelton, promised to keep an eye on the account.

A few days later, on May5, an unusual deposit of $4,358 was made into Karl's checking account. The funds came from Chase. "It caught my eye because it was an electronic credit card transfer," says Shelton. "That's not something you see every day."

That night Karl was contacted by someone identifying himself as George Selembo, financial supervisor for kflogistics.biz. USA TODAY located another George Selembo, 55, this one a quality-control inspector in Greensburg, Pa., who had once been a victim of ID theft.

In 2003, a cyberthief electronically transferred $8,000 from Selembo's Citibank Visa credit card to an overseas account. An additional $2,500 was withdrawn from his First Commonwealth bank account. No one was arrested, though the money was insured. Selembo spent six months resolving the matter. "Now you're saying that someone may be posing as me?" Selembo said in a phone interview. "Wow!"

Frozen funds

Via e-mail, the supervisor calling himself George Selembo instructed Karl to "please withdraw the whole amount" and send $4,011 via Western Union to Andrey Jaremchuk in St. Petersburg, Russia. Karl could keep the rest as his pay.

"It set off an alarm. Something was definitely wrong," Karl says. "I didn't take any of the money. I knew it was time to call the police."

Karl contacted the Nevada County Sheriff. Shelton, his banker, froze the $4,358. That triggered an acrimonious e-mail from Selembo.

"What?!!?? Give me the bank's(sic) manager phone. How long do they plan to keep your money frozen???" Selembo said in an e-mail to Karl on Friday, May6.

On Monday afternoon, May9, a male caller reached Shelton on the phone. The banker doesn't recall how the caller, who spoke with a heavy accent, identified himself. The caller claimed to have been cheated out of $4,300 by Karl and asked Shelton to return the funds. Shelton advised the caller to file a police report — and never heard from him again.

The next day, Karl received a final e-mail from Selembo: "I tried calling you a LOT of times. Reached only voicemail. When will you be home?" Karl turned the e-mail over to authorities.

"They made it clear they wanted the money withdrawn,"

Don't be a mule

Authorities advise taking these precautions to avoid being drawn into a reshipping scam:

- Be wary of advertisements and websites pitching home-based jobs for mail managers or shipping clerks.
- Insist on communicating with your prospective employer by phone or in person. Be wary of company officials who communicate exclusively via e-mail, particularly if the correspondence has poor grammar and spelling.
- Never e-mail or fax your driver's license number, Social Security number or other sensitive information — or anything with your signature — until verifying an employer's legitimacy.
- In online chat rooms, be wary of people who seek to quickly bond with you, then request your help with reshipping duties.
- When in doubt, contact the Federal Trade Commission or Better Business Bureau for guidance.

Sources: FBI, U.S. Postal Service

a nervous Karl recalls. "It began to freak me out. The tone of the messages was more threatening. I just wanted them to leave me alone."

The $4,358 remains frozen in Karl's Bank of America account pending a request from Chase, the bank that made the credit card transfer, for its return, says Shelton. "If they don't ask for it back, it's going to stay there forever," he says.

Chase declined interview requests. "Chase in addition to other banks and merchants are working with law enforcement and can't comment on this because of an ongoing investigation," said spokesman David Chamberlin.

Still useful

Kflogistics.biz wasn't done with Karl. In late April, he had begun receiving letters intended for online banking customers from all around the nation. The letters — account statements, notices of credit limit increases and discrepancy warnings — kept coming through June, long after Karl broke off communications with Birman and Selembo.

Karl was still useful: They could use his mailing address as a drop point for account statements linked to hot accounts. Often, the reshipper will change a billing address to a mule's, then ship goods to that mule to make it seem as if the card holder is ordering goods for himself, says Luehr, the former prosecutor.

One letter Karl received shed light on how the $4,358 credit card transfer was executed. The letter, dated May5, was a notice from Chase to Visa card holder Ryan Sesker of Des Moines, Iowa. Chase notified Sesker that his online request for a credit limit increase to $5,000 from $3,500 was approved.

But Sesker never made such a request. In fact, he says, he rarely used his Chase Visa card. The last two transactions came in early 2004, when he made online purchases of a computer printer and a Valentine's Day gift. By March 2005, Sesker had paid the balance down to zero, so the account wasn't at the top of his mind.

Sesker, who works as a banking loan officer, didn't know his account had been broken into until he was contacted by USA TODAY.

Upon notifying Chase of the break-in, Sesker learned someone had not only changed his billing address but also the date of birth and mother's maiden name associated with his account. About a week after Chase approved the credit limit boost to $5,000, the bank approved an electronic credit card transfer of $4,300 to a different account — the same kind of transfer that moved $4,358 from a Chase credit card account into Karl's Bank of America online checking account.

Chase declined to tell Sesker who the funds were transferred to. The bank indicated he will not be held responsible and asked him if he would like a new Visa credit card number. Sesker declined. Had he not noticed the breach for a couple of months, Sesker's credit might have become tainted.

"They probably would have been sending delinquency notices and collection letters to the wrong address," says Sesker. "I would never have known until the collection agencies tried to track me down."

Discussion

- What is a "mule." What are the two main functions of a mule?
- How do some Internet thieves avoid detection from banks and the FBI?
- How is the FBI fighting cybercrime? What hurdles does the agency face as it tries to protect consumers from fraud?
- How do reshipping operations work? What tactics do reshipping groups use to appear legitimate?
- When did "Karl" decide to contact authorities about kflogistics.biz? In your opinion, did he have cause to doubt the organization's legitimacy before then? Why did Karl continue to receive account statements and other correspondence even after he stopped working for kflogistics?
- Why might a reshipping "job" appeal to a young person? How can a teen ensure that she or he doesn't become an unwitting collaborator in a shipping scam?

Activity

To protect yourself and your information online, you must learn how to distinguish legitimate sites, e-mails, instant messages, etc. from dubious ones. (Remember: It's always best to err on the side of caution.) The graphic organizer on the following page will help you think about and internalize these distinctions. Using information from the article, www.staysafeonline.org and your own experiences, describe the characteristics of suspicious and legitimate websites, e-mails, etc., as listed on the following page. Then, discuss your graphic with a peer group, and add any information you may have overlooked. Finally, post the page near your computer as a reminder to be cautious online.

STOP. THINK. CLICK.

Describe a suspicious ...

Describe a legitimate ...

website

e-mail

pop-up window

instant message

employment ad

website

e-mail

pop-up window

instant message

employment ad