BusinessWeek

Close Window

JANUARY 9, 2006

INVESTIGATIVE REPORT

Gold Rush

Online payment systems like e-gold Ltd. are becoming the currency of choice for cybercrooks

Crime courses through the internet in ever-expanding variety. Hackers brazenly hawk stolen bank and credit-card information. Pornographers peddle pictures of little boys and girls. Money launderers make illicit cash disappear in a maze of online accounts. Diverse as they are, many of these cybercriminals have something important in common: e-gold Ltd.

E-gold is a "digital currency." Opening an account at www.e-gold.com takes only a few clicks of a mouse. Customers can use a false name if they like because no one checks. With a credit card or wire transfer, a user buys units of e-gold. Those units can then be transferred with a few more clicks to anyone else with an e-gold account. For the recipient, cashing out -- changing e-gold back to regular money -- is just as convenient and often just as anonymous.

E-gold appeals to "gold bugs": people who invest in the precious metal and believe money ought to be anchored to it. E-gold boasts that its digital currency is backed by a stash of gold bars stored in London and Dubai. But e-gold also appeals to savvy online crooks who want to move money quickly and without detection. American banks and conventional cash transmitters like Western Union are legally required to monitor customers and report suspicious transactions to the government. E-gold seems to go out of its way to avoid such obligations. Its operations are in Florida, but in 2000, its principals registered the company in the lightly regulated Caribbean haven of Nevis.

Law enforcement officials worry that the little-known digital currency industry is becoming the money laundering machine of choice for cybercriminals. On the evening of Dec. 19, agents with the Federal Bureau of Investigation and Secret Service raided the Melbourne (Fla.) office of e-gold's parent company, Gold & Silver Reserve Inc., and the nearby home of its founder, Douglas L. Jackson. Agents copied documents and computer files, but so far no charges have been brought. The Secret Service and the FBI declined to comment on the raid. Jackson has denied any wrongdoing, though the raid isn't the first indication that federal investigators view e-gold as a magnet for online misdeeds. The FBI separately is pursuing about a dozen probes in which e-gold appears as a "common denominator," a senior agent says.

The potential danger goes beyond e-gold. Investigators say other digital currencies are similarly used for corrupt purposes. All told, there are at least a dozen such services worldwide, based in places like Russia and Panama. Eight of them, including e-gold, claim to be backed by actual bullion. As a group, these firms do billions of dollars a year in transactions, according to Jim Davidson, a spokesman for the Global Digital Currency Assn. in New York. E-gold and its rivals make money by charging small percentage fees on those transactions.

Most of the law enforcement interest in e-gold involves alleged fraud and money laundering by its users. A tour of some outlaw

corners of the Internet illustrates why. One Web site called CC-cards -- where cyberthieves sell pilfered bank account and credit-card information -- often asks for payment via e-gold. Some sites pushing child pornography have dropped Visa and MasterCard recently in favor of e-gold, according to the National Center for Missing & Exploited Children, which tracks underage porn.

But U.S. officials have another concern: that e-gold and rival digital currencies could be used to finance terrorism. It's a notion the companies all reject.

SUBPOENA CENTRAL

The man behinD e-gold, Doug Jackson, is a tall, powerfully built former oncologist. A fan of the gold standard, Jackson, 49, became a pioneer in digital currency when he set out a decade ago to create what he describes as a private gold-based monetary system. He envisioned e-gold as a currency that would be accepted at Wal-Mart () while also permitting peasants from China to Peru to offer products at stable prices. "I thought there would be this flock of e-gold users, and I would be their messiah," he says. "It just didn't happen."

What did happen, according to law enforcement officials, was that a pack of felons flocked to Jackson's brainchild. Sitting in an undecorated conference room in the Melbourne office three months before the federal raid, he acknowledged that he had a "six-inch pile" of subpoenas from such agencies as the FBI, the Securities & Exchange Commission, and the U.S. Postal Inspection Service -- all seeking information about some of his more suspect customers. Investigators say Jackson may have begun his quirky business with innocent intentions. But in recent years he has turned a blind eye, the officials say, to mounting evidence that e-gold has attracted a seamy clientele. The federal raid suggests that agents are intensifying their focus on e-gold and its potential criminal liability.

Jackson didn't respond to messages after the raid. But earlier, he denied vehemently that he has looked away from crime. He said he responds as quickly as possible to official inquiries. He acknowledged, though, that his staff of 15 includes only one in-house investigator who struggles to keep up with all those subpoenas. E-gold has about 1.2 million funded accounts through which transactions worth $1.5 billion were conducted in 2005, he says. As for the idea that he should systematically monitor customer identities and money flows, he argues that's not his job: "We don't validate because we're unlike any other system."

Federal officials reluctantly confirm this loophole: E-gold and other digital currencies don't neatly fit the definition of financial institutions covered by existing self-monitoring rules established under the Bank Secrecy Act and USA Patriot Act. "It's not like it's regulated by someone else; it's not regulated," says Mark Rasch, senior vice-president of the Internet security firm Solutionary Inc. and former head of the Justice Dept.'s computer crime unit. The Treasury Dept.'s Financial Crimes Enforcement Network (FinCEN) is studying ways to close the regulatory gap. Meanwhile, U.S. officials say e-gold and similar companies should voluntarily do more to deter crime.

Started in 1996, e-gold was part of an early wave of Internet payment systems that converted conventional money into a Web currency. Most of those pioneers soon flopped, because consumers resisted paying fees to get Web cash. Others, such as PayPal, now a unit of online auction giant eBay Inc. (), evolved into credit-card processing services.

E-gold and a handful of rivals, including one called GoldMoney, were different. Their founders believed that tying monetary exchange to a strict gold standard would achieve greater economic stability. The Internet provided a ready venue for gold bugs the same way that it offered a soapbox to adherents of every other strain of thought. Jackson, an Army veteran and a graduate of Pennsylvania State University's medical school, was practicing oncology in Melbourne in the mid-1990s when he began reading about libertarianism and monetary theory. The married father of two adopted boys began to change his thinking. He scoured the works of libertarian novelist and philosopher Ayn Rand and was impressed by economist Friedrich A. Hayek's *The Road to Serfdom*, an influential 1944 condemnation of government control of the economy. "It looked like a lot of the suffering of recent centuries -- some of the scale of wars, some of the economic dislocations -- could be traced back to credit cycles. And credit cycles could be traced back to monetary manipulation" by governments, Jackson says. "I was very moved by it."

INTELLECTUAL CONVERSION

Gold, he concluded, was the cure. The U.S. stopped tying the dollar to a fixed amount of gold in 1971. But Jackson and a friend, attorney Barry K. Downey, decided to start what amounted to their own gold-backed currency. Jackson liquidated retirement accounts and sold his medical practice to help raise an initial $900,000. A former colleague noticed him working on computer code around the clock at his stand-up doctor's desk. He often forgot to eat and lost weight. Along the way, he stopped attending church. Jackson confirms all this but stresses that he continued to provide excellent care for his patients until he bowed out of medicine completely in 1998.

In a series of interviews with Jackson, his statements about e-gold swing from grandiose to resigned. "We want e-gold to be

recognized as a privately issued currency and to be treated as a foreign currency" by the U.S. and other governments, he says at one point. But e-gold's offices don't conjure up images of a grand central bank. Jackson, who during one interview wore neatly pressed slacks and a yellow-striped shirt, runs his currency from a Spartan suite on the third floor of a Bank of America () building.

Online currencies are patronized by software companies and other small businesses. Jackson says that the fees he charges customers -- for converting real money to e-gold, administering accounts, and doing transfers -- generated about $2 million in revenue in 2005 for e-gold's parent company, Gold & Silver Reserve, which he also controls. The operation turns a profit, he adds, but he won't say how much.

Mark Jeftovic considers himself a big fan of digital currencies -- but one now skeptical about e-gold. The founder of easyDNS Technologies Inc., an Internet domain name registrar in Toronto, he started accepting e-gold as payment in 2003. Jeftovic believes that digital currencies will minimize the harm of government-induced inflation. But in early 2005, investigators from the Royal Canadian Mounted Police visited easyDNS seeking information about cybercriminals allegedly using the registrar's services. It turned out that some of the suspects had paid Jeftovic's company via e-gold, he says. Angered by the police scrutiny, Jeftovic now plans to offer rival digital currency GoldMoney in addition to e-gold. "I like the digital currency and e-gold economy, and I want to support it," he says. "But you have to run a cleaner shop than this."

The RCMP didn't respond to requests for comment. Jackson says he wasn't aware of Jeftovic's concerns or the RCMP investigation. He says that e-gold responds as quickly as possible to inquiries from law enforcement agencies and readily provides them with user names, account numbers, and transaction histories.

A number of gold buffs and some law enforcement officials see GoldMoney as a reputable alternative in the digital currency field. Based in the British Channel island of Jersey, GoldMoney is run by James Turk, a precious metals trader and former Chase Manhattan banker. He says that his company requires new customers to mail in copies of identity documents and then checks the data against lists of suspected terrorists and money launderers. The accounting giant Deloitte & Touche annually audits its gold holdings and security measures.

E-gold's Jackson says those steps are expensive and unnecessary. OmniPay, an affiliate of e-gold, is one of more than a dozen "digital currency exchange agents" that handle the conversion of conventional currency into e-gold. Jackson says that to authenticate users' identities, OmniPay sends them a special code via e-mail and conventional mail. But users aren't required to prove their identity, so it isn't clear what this accomplishes. Jackson says that his lone in-house investigator looks for obvious fraud, such as a customer using "China" as his only address.

Some of e-gold's customers have been unsavory. Omar Dhanani used e-gold to launder money for the ShadowCrew, a cybercrime gang with 4,000 members worldwide, according to an October, 2004, affidavit by a Secret Service agent. Based in a stucco house in Fountain Valley, Calif., Dhanani used his PC to hide the money trail from the sale of thousands of stolen identities, bank accounts, and credit-card numbers, the government said. Accomplices sent him Western Union () money orders, which, for a fee, he filtered through e-gold accounts. On Oct. 4, 2004, Dhanani, 22, who used the nickname Voleur -- French for thief -- boasted in a chat room that he moved between $40,000 and $100,000 a week. He pled guilty in November to conspiracy to commit fraud and faces up to five years in prison.

"GOOD FENCES"

E-gold's Jackson says the company was never contacted by the Secret Service regarding Dhanani and had no duty to sniff him out. E-gold's outside attorney, Mitchell S. Fuerst, calls statements in the Secret Service affidavit alleging that e-gold was used to facilitate illegal activity "nonsense." Fuerst argues that the responsibility for policing the identity and activities of e-gold account holders lies with the banks and other regulated institutions from which money is transferred into e-gold's system. Jackson goes further, insisting it's impossible to launder money through e-gold -- a contention that law enforcers say is contradicted by the Dhanani case and others.

Jackson has made no secret of his desire to avoid U.S. government scrutiny. In 2000, he and his partner Downey registered e-gold Ltd. in Nevis, hoping the maneuver would add another layer of insulation from U.S. regulation. Jackson concedes that e-gold has existed in Nevis only as "a piece of paper." Its parent administers e-gold services from the Melbourne office; the operation's computer servers are in Orlando. Jackson says he chose the tiny island because registration there is inexpensive, and the government follows well-established British commercial law. Nevis is also known for lax financial regulation. Referring to his desire to create legal distance from U.S. officials, Jackson says: "There's an element of good fences make good neighbors."

On Dec. 5, two weeks before the federal raid in Melbourne, the Nevis Financial Services Regulation & Supervision Dept. posted a notice on its Web site that e-gold had disseminated "misleading information" about its legal status. Nevis officials say that the company was removed from the island's corporate registry in July, 2003, for failure to pay the annual registration fee of $220. Jackson

didn't respond to questions about this.

Back in the U.S., e-gold has tried to shield itself semantically, avoiding basic banking terms such as "deposit" and "withdrawal" that could increase its risk of being categorized as a regulated financial institution. E-gold calls such transactions "in-exchange" and "out-exchange." Jackson says: "It's not a desire to be tricky. It's a desire to be accurate. It's important not to be misconstrued as a bank."

Whatever its legal status, e-gold's usefulness to scam artists was colorfully illustrated by E-Biz Ventures, which allegedly portrayed itself as a Christian-influenced organization that offered investors returns as high as 100%. E-Biz' proprietor, Donald A. English of Midwest City, Okla., allegedly highlighted his reliance on e-gold to appeal to victims' fear of the federal government and their desire for anonymity. E-Biz investors opened e-gold accounts and transferred funds to accounts controlled by English. He shifted e-gold among more than 25,000 accounts, using new investors' money to pay off some older ones. The scam took in $50 million before the SEC shut it down in 2001. Investors lost $8.8 million. Later prosecuted in federal court in Oklahoma City, English pled guilty to wire fraud and last May was sentenced to five years in prison.

Jackson says that when subpoenaed by the SEC in the civil part of the E-Biz case, e-gold supplied transaction data. A Jackson aide worked closely with investigators in the civil case. "They responded timely to every request for assistance," says Chris Condren, E-Biz' court-appointed receiver.

Evidence of e-gold's suspect following is found on numerous Web sites. A contributor to Cannabis Edge, a site for marijuana growers, has provided advice on how to employ e-gold and two other digital currencies -- WebMoney and NetPay -- to hide illicit proceeds "beyond the reach of U.S. pigs." E-gold in particular "has strong security," is "easy to use, and is anonymous," said the writer, who used the name Bill Shakespeare. (Moscow-based WebMoney and NetPay, which is based in Panama City, Panama, both deny any wrongdoing.)

In addition to its abundant offerings of stolen financial data -- with payment frequently sought via e-gold -- the site CC-cards carried a message in November from a hacker using the name HellStorm. He advertised that for a 5% fee, he would set up and fund e-gold accounts for those who are in a hurry to do business and want to shield their identity. Users of CC-cards can make donations for the upkeep of the site by clicking on a link that connects to an e-gold account. (E-mails seeking comment from CC-cards and Cannabis Edge weren't answered.)

Jackson says that he wasn't aware that e-gold was being recommended or used on outlaw Web sites until he was so informed by *BusinessWeek*. The company has since blocked the CC-cards donation account, he says. There is little the company can do about such situations, Jackson contends, unless law enforcement brings them to e-gold's attention. Once informed, "we can set a value limit to prevent an account from receiving further payments," he says. "We can identify if there is a constellation of accounts controlled by the same miscreant." Jackson adds: "If we get an appropriate court order, we can monitor and assist in a sting that freezes value."

The danger of Web sites like CC-cards that are fueled in part by e-gold became very apparent to Kimberly S. Troyer. Her identity went up for sale there last September. Among the 22 items CC-cards put on the block: her checking account number at Bank One (), driver's license number, Social Security number, birth date, and mother's maiden name. The price for all that: $30 of e-gold. Informed of the offer by *BusinessWeek* in December, Troyer, a 33-year-old accounting student at Davenport College in South Bend, Ind., is changing all of her identity documents. She believes she escaped without losing any money. But someone hijacked her e-Bay account and changed the address to one in China so that it could receive payments from the sale of iPods Troyer didn't own. "It makes me sick to my stomach," she says. Jackson says e-gold can't do much about such cases until he's formally alerted by the government.

There is one crime, however, to which Jackson has reacted more aggressively: child pornography. In August, he attended a conference in Alexandria, Va., organized by the National Center for Missing & Exploited Children. The center is trying to enlist banks and credit-card companies in a crackdown on payment schemes used by child porn Web sites. "There are fewer and fewer sites with Visa -- and more and more with e-gold," says the center's chief executive, Ernest E. Allen. The center has a policy of not publicly identifying child porn sites it tracks. Jackson says he was appalled to find e-gold on the list of institutions used by the porn sites. He provided the center with instructions on how to seek e-gold records, and the group says it is pleased with e-gold's cooperation.

Daniel J. Larkin, head of the FBI's Internet Crime Complaint Center, says that in recent years, e-gold has hidden behind "a plausible-deniability fog." Now the fog may be lifting as the subpoenas pile up and federal agents begin to examine what they confiscated in their Dec. 19 raid. The Internal Revenue Service is separately auditing e-gold's parent, and Jackson says e-gold has voluntarily agreed to cooperate with an IRS review of its procedures for preventing money laundering. The IRS declined to comment.

TERROR TOOL?

Before the recent raid, Jackson said that responding to subpoenas and other government inquiries has been distracting and expensive. Although he emphasized that e-gold isn't obliged to monitor its clientele, he said that he could have paid more attention to vetting account holders were it not for the outside interruptions. He added that he plans to switch from an account-based log-in system to a user-based one to monitor customers more closely.

The worst-case scenario, so far undetected by officials, would be the use of e-gold by financiers of terrorism. Experts on terrorism funding note that digital currencies resemble the money-changing system known as hawala, which Middle Eastern terrorists have used. A customer gives money to a hawala service, which then telephones a similar service in another city or country that doles out money to a designated recipient. Many hawala outfits have been shut down since September 11, making digital currencies a logical next step, says Phil Williams, a professor of international affairs at the University of Pittsburgh and consultant to the United Nations on terrorism financing. "At some point, this is going to be used" by terrorists, Williams says.

Jackson scoffs at this notion. "We are not bad guys, and the e-gold system simply does not pose an undue risk for usage for terrorist purposes," he wrote in an e-mail on Jan. 20, 2005, to AUSTRAC, Australia's anti-money-laundering regulator, which was looking generally into potential terrorist use of digital currency.

But e-gold attorney Fuerst said in early December that the company quickly complied with requests in 2005 from Russian law enforcement and the FBI for records connected to a would-be terrorist in Russia. This person allegedly threatened to "blow something up," Fuerst said, unless a ransom was paid into his e-gold account. The FBI and the Russian Interior Ministry declined to comment.

This month's raid could signal serious trouble for e-gold. But cybercrime experts predict that if the company falters, nefarious business will simply transfer to other digital currencies, especially ones based in countries that have lax law enforcement. Amir Orad, executive vice-president of cybersecurity firm Cyota, says that putting e-gold out of business "would not stop anything."

By Brian Grow, with John Cady, Susann Rutledge, and David Polek in New York