Well-connected Internet users who distribute secret or sensitive information without revealing their names are playing havoc with national laws. **Charles Arthur** reports

Identity crisis on the Internet

Invasion: Erlich (third from left) had his home searched by police and lawyers representing the Scientologists

IN THE past few weeks several citizens of cyberspace have heard an unfamiliar sound—the knock of uninvited guests. The arrest of Kevin Mitnick, alleged hacker extraordinaire, was widely reported by the world's media. Less coverage followed two other incidents. In Glendale, California, a few days before Mitnick's arrest, lawyers from the Church of Scientology accompanied by police officers presented a former member of the church, Dennis Erlich, with a warrant to search his apartment. On 8 February, at the request of Interpol, Finnish police served a similar warrant on Johan Helsingius, who runs a computer in Helsinki linked to the Internet.

Mitnick may have stolen the headlines, but the actions against Erlich and Helsingius have sparked far more discussion on the Internet because they arise from a piece of technology called an anonymous remailer, which companies and governments see as a growing threat. Their fear is that these devices, together with encryption programs, will undermine long-established laws designed to protect the ownership of information and control its spread. With this combination of technologies, people will be able to publish any confidential information, without the fear of being caught.

Untraceable contacts

An anonymous remailer is simply a computer connected to the Internet that forwards electronic mail or files to other addresses on the network. But it also strips off the "header" part of the messages, which shows where they came from and who sent them. All the receiver can tell about a message's origin is that it passed through the remailer. Some remailers also allocate each sender an "anonymous ID", rather like a PO box number, which it stores with the sender's address so that any replies reach them.

These anonymous remailers were invented by security experts interested in whether it was possible to send a message on the Internet which could not be traced back to its source. As soon as the first ones were built, though, people found a more pragmatic use for them: to send messages to bulletin boards about subjects so sensitive that they did not want their names known. People with unusual sexual tastes make good use of remailers, as do the victims of sexual abuse.

But the use of remailers can also make it impossible to enforce national laws. How can copyright be protected, for example, if anything that can be scanned into a computer can be broadcast anonymously to millions over the Internet? How can a judge ensure that prejudicial information does not leak from a court if anyone in the public gallery can distribute those details from the nearest terminal without fear of being caught? The inability to trace the source of information may foil the police on the trail of a pornographer, and leave companies struggling to deter a disgruntled employee or client from revealing commercial secrets.

Examples of all these scenarios have taken place recently. The scientologists accuse Erlich of posting material to which it claims the copyright on one of the Internet's bulletin boards, or "Usenet newsgroups". Erlich denies the charge, saying he made "fair use" of the information within the terms of the law. The church's lawyers are also pursuing messages that were routed through Helsingius's anonymous remailer. No clear evidence exists about the sender. So, through Interpol, the lawyers asked the Finnish police to search Helsingius's property, including his remailer, in order to locate the suspect from its database. No case has yet come to court.

Similarly, in Britain, when Rosemary West was charged with 10 murders last month, details from a pre-trial hearing were posted anonymously to a newsgroup for all to read. Yet no British newspaper or magazine could have published them without being held in contempt of court.

As for pornography, newsgroups abound with obscene pictures sent through remailers. And last year RSA Data Security, a cryptography company based in Redwood City, California, found that software which laid bare its RC4 encryption algorithm had been posted—via anonymous remailers—onto the Internet. The company was appalled. It had regarded RC4 as secret.

The combination of anonymous remailers and encryption programs—of which scores

are freely available—raises particular concerns. With these technologies, people can confidently leave private messages in a public place—on a newsgroup, for example. Without a decryption key, these messages will look like rubbish.

Four Horsemen of the Internet

Correspondents could further cover their tracks by sending messages through chains of remailers. People often build up relationships in cyberspace without meeting, but by using cryptography and remailers they might not even know who it is they are dealing with. One might request military or industrial secrets; the other would send them, along with the number of a Swiss bank account for the payoff. If the police noticed the messages and were able to crack the code and trace one of the pair, that person would be unable to name the other, even if he or she wanted to.

Some are worried by this aspect of remailers. "They envisage them being used for what I call the Four Horsemen of the Internet. That is—terrorism, child pornography, money laundering and drugs," says Timothy May, a Californian cryptography and computing consultant. So, should remailers simply be closed down? Absolutely not, says May. "Just as privacy in hotel rooms should not be banned simply because a lot of crime—drug deals, plotting, sexual perversity—happens in hotel rooms," he says.

Helsingius agrees. "These servers enable safe discussion of sensitive issues, such as reporting violations of human rights. They are vital for support of freedom of expression," he says. "These servers are used by people all over the world who are under pressure or persecuted, or who want to discuss their personal problems and sufferings."

There are 27 publicly listed remailers on the Internet, though the worldwide total is closer to a hundred. Helsingius's, which is one of the oldest, was only set up in 1992. Since then, 200 000 people have sent mail through the machine. At present it deals with more than 7000 messages a day.

Politicians who would like to keep an eye on this and other traffic on the Internet face an unenviable task. Ian Taylor, Britain's technology minister, admitted recently that it is virtually impossible for governments to say what can and cannot be done on the Internet (This Week, 27 February). Chris Smith, a Labour MP who is helping to frame his party's strategy on electronic information, is also at a loss over remailers. "There are clear benefits to remailers, for support groups and so on, but also dangers in that criminal activities could be undertaken. I'm not sure there is any system that can preserve the benefits but avoid the downside," he says.

Shutting down remailers altogether is a very unlikely prospect. It would provoke a storm from people who use them for legitimate reasons. In addition, every country in the world would have to adopt the law, because the nature of the Internet means that wherever a remailer exists, it can be used.

Governments trying to legislate on anonymous remailers have found that for every legal twist they think up there is already a technological turn that evades it. What about a law dictating that remailer operators must know the source of a message? May responds: "Send it via somebody who 'quotes' your message, which is encrypted." What about refusing any message containing encryption? Sometimes you cannot tell when a message is encrypted. A text message, for example, can be included in a digitised picture by altering the least significant bits of its pixels. It is the electronic equivalent of the microdot: what seems like a holiday snap might contain the blueprint of a building or a bomb.

On encryption, Smith favours a system where the only programs permitted would be those that the government knew it could unscramble. If it suspected that a crime was being or about to be committed, it could then seek a court order to eavesdrop on suspects. "That's one of the things we would like to look at," he says.

But, again, the technology eludes such control. The posting of the RC4 algorithm means that anyone determined enough could create their own, practically uncrackable, code. And that code can pass across national borders as easily as a phone call. Encryption programs such as PGP are already freely available over the Net.

Taylor identified laws on the protection of intellectual property as already under threat from developments on the Internet, and in need of international action. May believes the time is coming when the whole notion of ownership of information will need to be rethought.

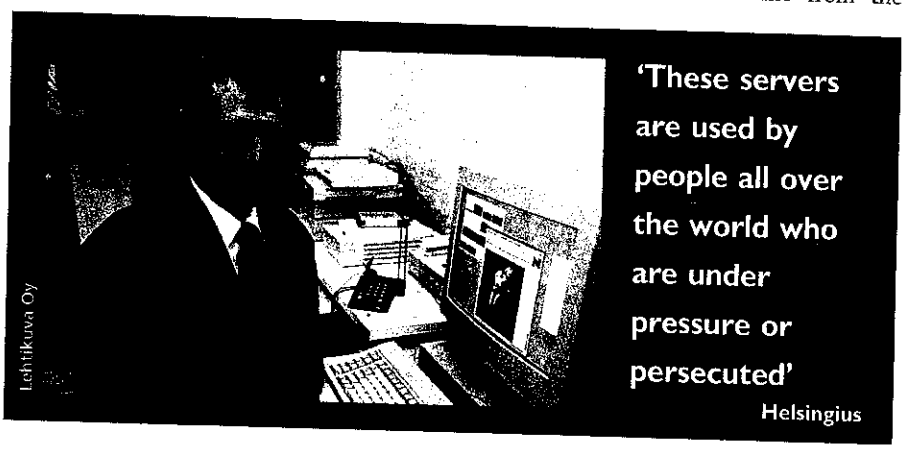
He sees parallels between the efforts of governments and companies to keep information to themselves with those of medieval guilds. "Medieval guilds believed that they owned the knowledge of how to shoe a horse, for example," he says. "That's very like the modern system of patents and copyrights." But the guilds fell victim to the arrival of printing and the spread of literacy, because knowledge could be passed freely to any number of people.

There is even a modern example of how the Internet can make an impact on "restricted" information. In the US, there are laws against selling locksmiths' tools to the public. But one newsgroup has seen anonymous postings of lock-picking methods. When the editor of a locksmith journal plugged into the Internet last year, he was appalled to find trade secrets being openly discussed. May is unimpressed. "In the long term, I think 'copyright' as we know it today is dead, just as the information 'owned' by the guilds ceased to be owned by them after several decades or so of books being available," he says.

So how can those aiming to protect existing laws defend them? Brad Templeton runs an electronic news service called ClariNet, which distributes articles to readers over the Internet, each of whom pays a subscription fee. Occasionally, ClariNet's revenue is threatened when an article has been reposted anonymously. "It happens rarely, and we do have ways of dealing with it," says Templeton. "We have contracts with all our subscribers that make such posting not just a copyright violation but a breach of contract. The operators of remailers have no interest in having their remailers used for illegal activity and usually are quick to pull the access of anyone who tries this."

Indeed, the most likely source of regulation for remailers will come from the operators themselves. For example, Matthew Ghio, a student at Carnegie Mellon University, Pittsburg, who runs an anonymous remailer, refuses to forward mail to the White House because it might contain death threats, and he doesn't want the US Secret Service knocking on his door. Helsingius has vowed to fight any restriction placed on his remailer. But a code of conduct is evolving slowly.

In their way, the publishers and governments of today are probably no less powerful than the guilds and kings of the Middle Ages. And, like the printing press, the Internet is becoming so widely available as to be irresistible. The question now is whether the Internet will have as profound an impact as printing.



Los Angeles Times Photo

Lehtikuva Oy

Newark airport blackout exposes system flaws

By Thomas Hoffman
NEWARK, N.J.

Newark International Airport and its tenants were victimized twice last week — first by a construction gaffe that cut power cables feeding the airport's main terminals and then by poor disaster recovery planning that caught those affected with their pants down.

Last Monday, a construction crew driving 60-ft steel beams into the ground for a new parking deck inadvertently cut three 27kVA power cables, knocking out power to the airport's three main terminals.

They're grounded!

DATE OF INCIDENT	SYSTEM/AIRPORT AFFECTED	CAUSE
Jan. 15, 1990	Nationwide AMR Sabre System	Software error
Jan. 4, 1991	New York Air Traffic Control	Network crash
June 10, 1991	Washington Air Traffic Control	Power outage
Oct. 16, 1992	New York Air Traffic Control	Software error
Feb. 28, 1994	Denver International Airport	Power surge
May 19, 1994	Detroit Metropolitan Airport	Hardware error

Source: Contingency Planning Research, Inc., White Plains, N.Y.

The blackout, which occurred at 8:30 a.m., forced the airport to shut down at 5 p.m. while Public Service Electric & Gas Co. utility crewmen worked through the night to install a 100-ft loop of cable to bypass the three damaged lines. Power was restored to the airport by 5 a.m. the following morning.

During the blackout, airline and rental car reservation systems in the terminals went down, forcing airlines to divert passengers to other East Coast airports and costing them millions of dollars in lost sales.

A spokesman for The Port Authority of New York & New Jersey, which owns and operates the airport, said the agency has called for a formal review of the incident, including a cost projection. The preliminary report is due later this month.

Puzzling issues raised

The incident raised several questions about the airport's tenuous infrastructure, such as why the hub's primary and auxiliary power sources are laid side by side in the same conduit.

"If you run cables in the same conduit, it's less expensive, but IS people learned years ago that if you have a primary telecommunications path and a backup path, you don't put them in the same physical location," explained Ken Brill, president of ComputerSite Engineering, Inc., a Santa Fe, N.M., disaster recovery consultancy.

In addition, the power configuration at Newark was put in place 25 years ago, long before diversified power and telecommunications feeds had become de rigueur. "The cost to diversify those cables in the original construction process would have been minimal," added Brill, founder of the Uninterruptible Uptime Users Group.

Along with its infrastructure problem, the airport seemed to have inadequate backup power supplies, such as uninterruptible power supplies and diesel generators, to keep the entire facility humming.

What remains unclear is what, if any, actions the information systems organizations of the affected airlines might take to prevent similar occurrences in the future. Requests for interviews with IS executives at Delta Air Lines in Atlanta and Continental Airlines in Houston were declined or went unanswered last week.

Newark Airport *lost millions of dollars in sales during a recent blackout that shut down its reservation systems*

During the crisis, airline agents whose computer reservation terminals went black after the power outage were left scrambling to direct passengers to New York's La Guardia Airport and John F. Kennedy International Airport as well as Philadelphia International Airport.

USAir agents at Newark, for instance, ended up calling the airline's main reservation centers in Syracuse, N.Y., and Charlotte, N.C., in an effort to redirect stranded passengers. The Arlington, Va.-based carrier then manually processed customers through Newark and doubled-up passengers on some of its flights, said Millie Valerio, a USAir customer service representative.

The incident resulted in 616 of Newark's 1,400 flights being canceled or rerouted to airports as far-flung as Bangor, Maine, and Chicago, said a spokeswoman for the Federal Aviation Administration in Washington.

Ex-Officer Admits Credit Card Misuse

2/16/95

WHITE PLAINS, Feb. 15 (AP) — A former correction officer admitted today that he used stolen credit cards to buy sheets and a camcorder at a Yonkers department store, District Attorney Jeanine Pirro of Westchester County said.

The former officer, Kenneth Watford, 26, of New Rochelle, pleaded guilty to an indictment that included counts of second-degree forgery and criminal possession of a forged instrument.

Ms. Pirro said that Mr. Watford, who had been a correction officer since November 1990, used the cards at a Bradlees store in Yonkers in December 1993.

The magnetic strips on the credit cards had been altered so that when the card was put through the register, a different account number was recorded on the receipt, Ms. Pirro said.

Mr. Watford, who had been earning $36,535 a year, resigned shortly after the incident, Ms. Pirro said.

Privacy vs. openness

Battle lines shape up over motor vehicle records

BY JAMIE PRIME

Early skirmishes

Federal legislation to restrict driver's license data is forcing the issues of stalking, privacy, and open records into the states.

- **Missouri** legislators recently rejected three bills aimed at closing DMV record.
- **Illinois** restricts the release of DMV data; press and insurance groups are exempt.
- **Maryland** press groups killed a bill that would have restricted driver's license data.
- **Minnesota** rejected a proposal to ban DMV data release; state already lets license holders provide an alternate address.
- **Wisconsin** allows license holders to have their personal information withheld when more than 10 records are requested at one time, in a measure aimed at increasing privacy from direct marketers; a bill to completely prohibit release was killed.
- **Connecticut** tightened its policies for releasing DMV data to the general public; press retains access through a business exemption.
- **California** was one of the first states to limit the release of driver's license data as a victims' rights measure.

Driver and motor vehicle records have helped track down airline pilots who have been convicted of drunk driving. They were instrumental in uncovering the identities of Florida Ku Klux Klan members. They are an important fact-checking resource for reporters. But now, they may be off-limits to journalists and the public.

In the strange workings of Congress, the new crime bill tells the states they can keep public records open only if they pass laws allowing individuals to keep them private. If the states fail to do so in the next three years, entire record banks will be shuttered from public view.

The key lies in the "opt out" provision of the driver's privacy protection section of the law. States that enact laws to let licenceholders "opt out" of public disclosure will still be able to sell or release the remaining drivers' records.

Still, the presumption is that the records be closed. With the emotional issue of stalking combined with the concern for privacy, the presumpion of openness will be a difficult sell.

"What I see with the DMV is a wolf in sheep's clothing," says Jane Kirtley, executive director of the Reporters Committee for Freedom of the Press. The legislation has been sold as a privacy and anti-stalking issue, she says, but "it doesn't do either."

The provision's sponsors, Sen. Barbara Boxer, D-California, and Rep. Jim Moran, D-Virginia, say the law is needed to protect stalking victims. Opponents—including SPJ and other press groups—contend that the bill, while well-intentioned, will not prevent stalking and will actually keep members of the public who have legitimate needs from obtaining department of motor vehicle records. As written, the law restricts the release of "personal information": photographs, Social Security numbers (in those states that still collect them as part of DMV records), names, addresses, telephone numbers, any information that "identifies an individual." Information about accidents, driving violations, and a driver's status is not affected by the bill.

Access surprises many in Congress

When the DMV provision was introduced last November, it was hailed in both houses of Congress as an effective way to prevent stalkers from obtaining personal information, as well as a means to counter abortion protesters who take down the license plate numbers of doctors and

patients at clinics. Congressmen expressed surprise and outrage that DMV records are public record in many states, and the legislation looked to be on its way to a quick passage.

Although Boxer's bill whipped through the Senate and was added to the omnibus Crime Bill without public hearings, SPJ and other concerned groups—most notably direct marketers and private investigators—were able to persuade Rep. Don Edwards, D-California, to schedule a hearing in the Judiciary Subcommittee on Civil and Constitutional Rights, ultimately inserting compromise language in Moran's House bill. Under the compromise, Moran included the opt-out provision. In turn, SPJ and five other media groups—the American Society of Newspaper Editors (ASNE), the Reporters Committee, the Radio and Television News Directors Association (RTNDA), the Newspaper Association of America (NAA), and the National Newspaper Association (NNA)—issued a joint statement calling the Moran version the least objectionable, but still supporting the principle of no restrictions on DMV records. At the hearings, SPJ Freedom of Information Chair Lucy Dalglish and Rich Oppel, Knight-Ridder's Washington bureau chief who also represented ASNE, emphasized the need for open records, but endorsed a mandatory opt-out as a workable compromise

Compromise better than loss

Considering the political climate favoring the bill, Dalglish says, the public was fortunate to secure the opt-out. Outright opposition to the bill would have been all but certain to fail.

Although other groups opposed to the bill—including the insurance industry, private investigators, and towing operators—were able to secure exemptions, the media coalition quickly rejected the idea on both philosophical and practical grounds. An exemption for journalists is "completely undesirable and unworkable," Dalglish explains. "Who's going to decide what a reporter is? It's the first step toward licensing of journalists—it's the old slippery slope argument." Additionally, a media exemption would have left out the general public, and too broad an exemption might have been unacceptable to the bill's authors.

Emotions overwhelm concerns

With worries about the safety of stalking victims driving the bill, opponents worked to distinguish their concerns from the emotional issue. "We're not in favor of stalkers. We're not in favor of people misusing drivers' records," says David Bartlett, RTNDA president. "We were concerned that an otherwise apparently noble bill would have—as is so often the case—an unintended harm to journalists."

Press groups contend that stalkers and others who want names, addresses, and phone numbers are driven enough to find the information through alternate means, such as real estate records, voters rolls, and city directories. Only a limited number of cases can be attributed the release of DMV data where the information could not readily be found through other public sources.

Besides, Dalglish says, legislation should target stalkers and not public information. "You should go after the underlying behavior," she says. "Information is neutral. If people are stalking, pass a law that targets stalkers."

Victims' rights groups offer compelling stories of stalking victims who have been tracked from state to state through DMV records, as well as the story of actress Rebecca Schaeffer, who was shot to death by an obsessed fan who obtained Schaeffer's address from an investigator who requested a copy of her driver's license.

While they recognize that halting the release of DMV records won't stop stalking, the groups say every bit helps. "We realize that we're not trying to close every possible loophole," says David Beatty, who testified before Congress as director of public affairs of the National Victim Center. "In some instances, those levels of marginal increments of safety can be the difference between life and death."

Journalists will still be able to work around the restrictions, Beatty predicts. "Any good investigative reporter will be able to find the information he needs. This is one small little piece—when you compare that increment of convenience for competent reporters, it doesn't match up with the risk of death for stalking victims."

Other groups, especially police organizations, joined in support of the bill on victims' rights grounds. "Why make it easy on [the stalkers]?" asked Don Cahill, legislative chair for the National Fraternal Order of Police. "They'll find a way, but there's no reason to make it easy for them."

Privacy vs. openness

While the stalking issue has attracted the most attention, the law also forces a collision. "We're trying to balance the right to privacy with the need to have access to that information," says Laura Murphy-Lee of the American Civil Liberties Union. Under the ACLU's analysis, the individual's interest in keeping license information private outweighs the public's interest in disclosing DMV records.

"The balance comes down in favor of openness," Dalglish says. "Some loss of personal privacy is the price you pay for living in this type of society."

Supporters of the bill on privacy grounds also include the Consumer Federation of America and the American Medical Association.

"There is so much personal data available through files of local motor vehicles—it needs to be secured," says Nancy Turner, public policy advocate for the National Coalition Against Domestic Violence. The Consumer Federation of America, a pro-consumer group that promotes privacy issues, opposes opt-outs "as a matter of principle," preferring an opt-in concept, where people must request that their license data be made public.

State arena next battleground

Even though the opt-out for members of the public—and the press—is law, those interested in freedom of information still have to convince states to enact opt-out provisions. For the first three years, states will be able to continue their existing policies for releasing DMV records. Then, the state will be able to release the drivers' license data to the public only with the license holder's written consent or if it has enacted an opt-out provision. Persons who illegally obtain or disclose DMV information will be subject to both civil and criminal penalties.

FOI groups have the opportunity to open restrictive state DMV policies. "The opt-

PROTECT YOUR GOOD NAME

Alteration. Forgery. Counterfeiting. There are many different forms of check fraud, but all can create the same problems for victims. Overdrafts. Bad credit ratings. Time and money spent clearing your name. What's more, the Supreme Court has ruled that if you do not take precautions to protect your checks, you may be held liable for the losses.

Below are seven tips for safeguarding your account:

Use Fraud-Evident Originals™ from Deluxe.

Reconcile your statement regularly.
You are responsible for discovering and reporting check fraud promptly. If you fail to do so, you may be held responsible for the losses.

Treat your checks like cash.
Don't leave them where they can be stolen. And don't think that a criminal needs your entire checkbook. Hundreds of copies can be made from a single check.

Don't use deposit tickets for notepads.
And shred or destroy all financial documents before disposing of them. This applies to anything with your account number including bank statements and extra deposit tickets.

Minimize the personal data on your checks.
If your driver's license number or social security number is printed on your checks, request that it be removed with your next reorder. These valuable numbers give criminals all they need to get fake I.D., credit cards and more.

If your checks are lost or stolen, take action.
Contact the office where your account is located. Request that they notify ChexSystems' "Lost or Stolen Check Hotline" immediately to prevent others from using your checks.

Mail your payments at the post office.
Don't leave checks lying in your mail box.

MAKE YOUR CHECKS TOO TOUGH TO ALTER

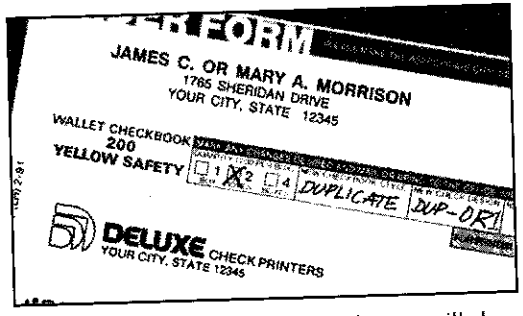
With crime on the rise in all aspects of our lives, it's not surprising that our checks are at risk as well.

Improvements made to color copiers and desktop publishing make it easier than ever to alter or counterfeit a check. In fact, the Federal Bureau of Investigation (FBI) reports an alarming increase in the number of check fraud cases over the last ten years.

The good news? Now you can enjoy the convenience of checkwriting with even greater peace of mind.

STOP FRAUD BEFORE IT STARTS

To order Fraud-Evident Originals™, write WAL-OR1 or DUP-OR1 on the reorder form included in your check package.



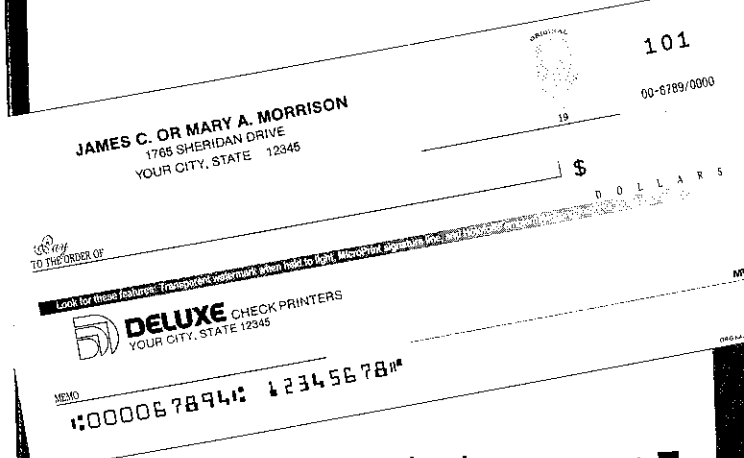
The price of the check package will be deducted from your account.

DELUXE

FOR PERSONAL ACCOUNTS

SECURITY ...IT'S ON YOUR MIND

IT COULD BE ON YOUR CHECKS



Introducing a new way to protect your checking account from fraud

FRAUD EVIDENT Originals™ FROM DELUXE

6 WAYS TO PROTECT YOUR ACCOUNT FROM FRAUD

Criminals want easy targets. When they see all the roadblocks these checks put in their way, they will be more likely to leave your account alone. The six key features integrated into every Fraud-Evident Originals™ check are shown and described here.

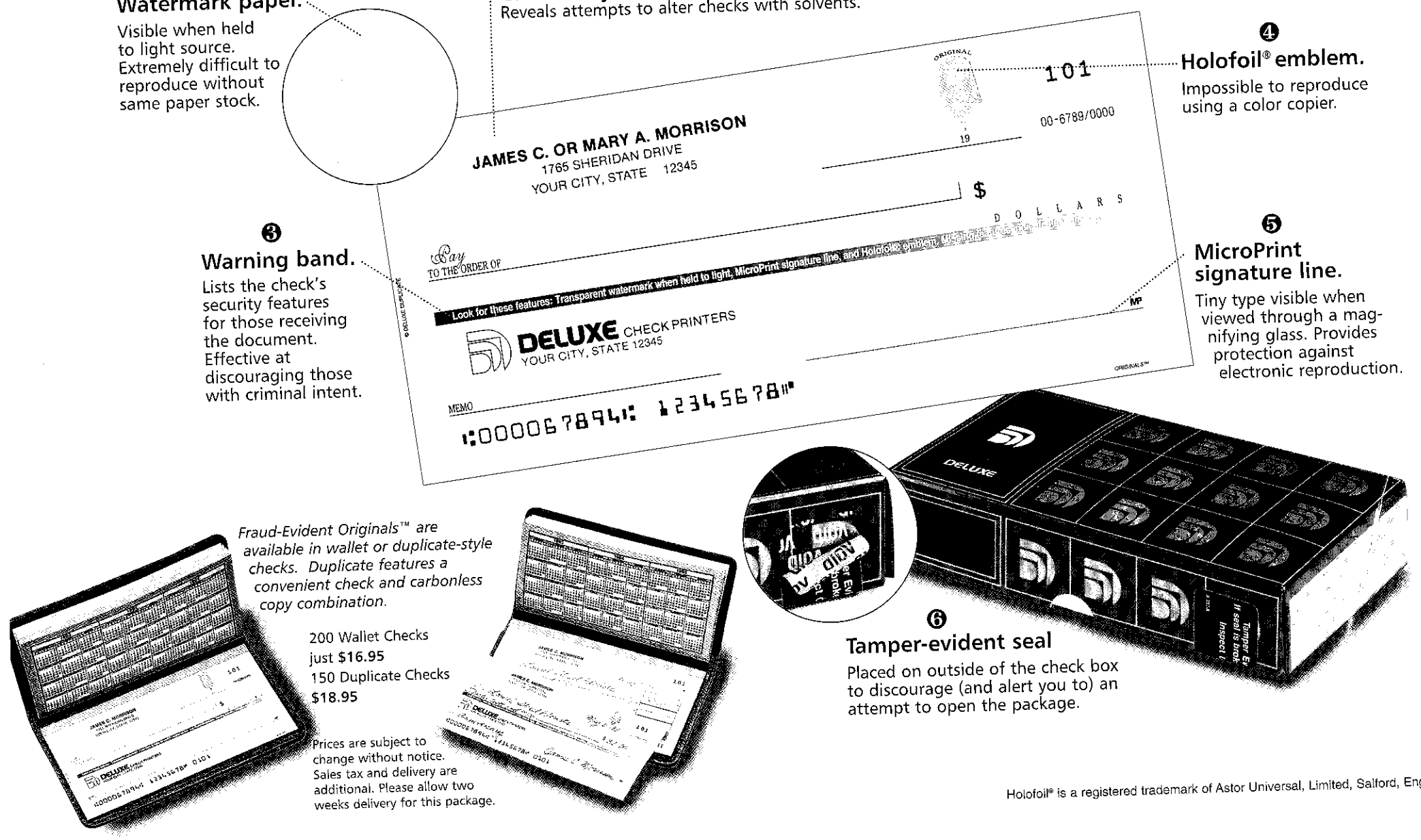
❶ Watermark paper.
Visible when held to light source. Extremely difficult to reproduce without same paper stock.

❷ Chemically sensitive paper.
Reveals attempts to alter checks with solvents.

❸ Warning band.
Lists the check's security features for those receiving the document. Effective at discouraging those with criminal intent.

❹ Holofoil® emblem.
Impossible to reproduce using a color copier.

❺ MicroPrint signature line.
Tiny type visible when viewed through a magnifying glass. Provides protection against electronic reproduction.



❻ Tamper-evident seal
Placed on outside of the check box to discourage (and alert you to) an attempt to open the package.

Fraud-Evident Originals™ are available in wallet or duplicate-style checks. Duplicate features a convenient check and carbonless copy combination.

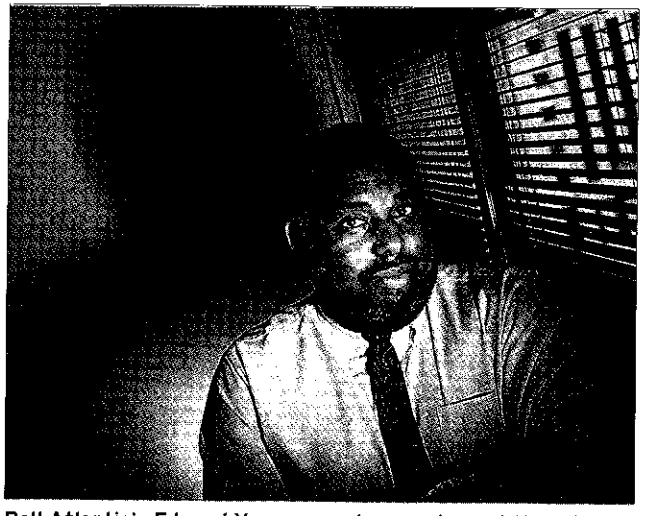
200 Wallet Checks
just **$16.95**
150 Duplicate Checks
$18.95

Prices are subject to change without notice. Sales tax and delivery are additional. Please allow two weeks delivery for this package.

Holofoil® is a registered trademark of Astor Universal, Limited, Salford, England

What You Don't Know

Privacy advocates can help navigate the mine-laden territory of consumer databases



Katherine Lambert

Bell Atlantic's Edward Young says hammering out the privacy code was a 'very difficult' process inside the company

By Mitch Betts

including people who like home-shopping services and watching movies, for example — are the same ones who expect some privacy for their on-line activities.

"To sell them, it's necessary to reassure them," says Humphrey Taylor, chief executive officer of the polling firm Louis Harris and Associates, Inc. in New York.

Of course, consumers are a pragmatic bunch. If you give them a big enough discount to divulge their life story and a say in how that information will be used, they will go along.

What consumers want is *advance* notice of the data collection and how it will be used, the poll found. They also want some control over the types and timing of the advertising messages, and they want to be able to review and correct their data profile.

Getting an edge

In fact, vendors who take a pro-privacy stance may get a competitive edge. "Fair information

the company. Typically, the tension is created by the fact that a company's marketers want maximum exploitation of consumer data to ensure the new venture will be a financial success.

By having a privacy advocate on board, the company gets an opposing viewpoint and some expertise about how other companies deal with privacy issues. "You certainly need to have people who will examine things from the customer point of view, not just the financial point of view," Young says.

The corporate privacy policies are not as strong as public interest groups might like, but they are a step in the right direction, says Marc Rotenberg, director of the Electronic Privacy Information Center in Washington.

"The good news is that these companies are becoming sensitive to consumer concerns and are trying to get ahead of the curve on this issue," Rotenberg says. "The bad news is that Washington hasn't caught up."

He says the Clinton administration task force that is drafting privacy guidelines for the National Information Infrastructure has "missed the boat," producing a weak-kneed set of guidelines that give consumers little or no protection.

Policy is no panacea

However, the Clinton administration did have the foresight to establish the task force and try to address the issue before some large-scale privacy disaster occurs.

Many companies have no comprehensive privacy code at all. They drift along with ad hoc decisions until some public relations crisis oc-

One way to make big bucks from the information superhighway is to compile detailed information on how consumers use on-line services. Then exploit this consumer "profile" for targeted marketing, promotions and cross-selling campaigns.

But in these privacy-sensitive times, that business model is also the fastest way to get blasted by politicians, the press, privacy advocates and the very consumers who services want to lure.

Just ask America Online, Inc., which was nailed last October by U.S. Rep. Edward J. Markey (D-Mass.) for trying to sell its subscriber data to the direct marketing industry.

"There is the potential to make a ton of money [selling on-line subscriber data], but this is an area where companies need to tread very carefully," warns Mary J. Culnan, an expert on consumer privacy at Georgetown University in Washington. By tracking every touch of a button, "these systems have an enormous potential for surveillance," she maintains.

Tiptoeing through minefields

Aware that a single slipup in the field of consumer privacy can be a public relations disaster, savvy companies are hiring consumer advocates and drafting confidentiality codes to navigate the privacy minefield.

The reason is not so much altruism as it is a marketing imperative. "Who will want to use our on-demand movies service if the list of movies they watch will be distributed elsewhere?" says Edward D. Young III, associate general counsel at Bell Atlantic Corp.'s Arlington, Va., office, which plans an interactive network.

Indeed, a recent public opinion poll found that the types of consumers who are prime targets for the new wave of interactive services — may get a competitive edge. "Fair information safeguards may be the very best marketing message for interactive services," says Alan F. Westin, a professor at Columbia University in New York and mastermind of the poll.

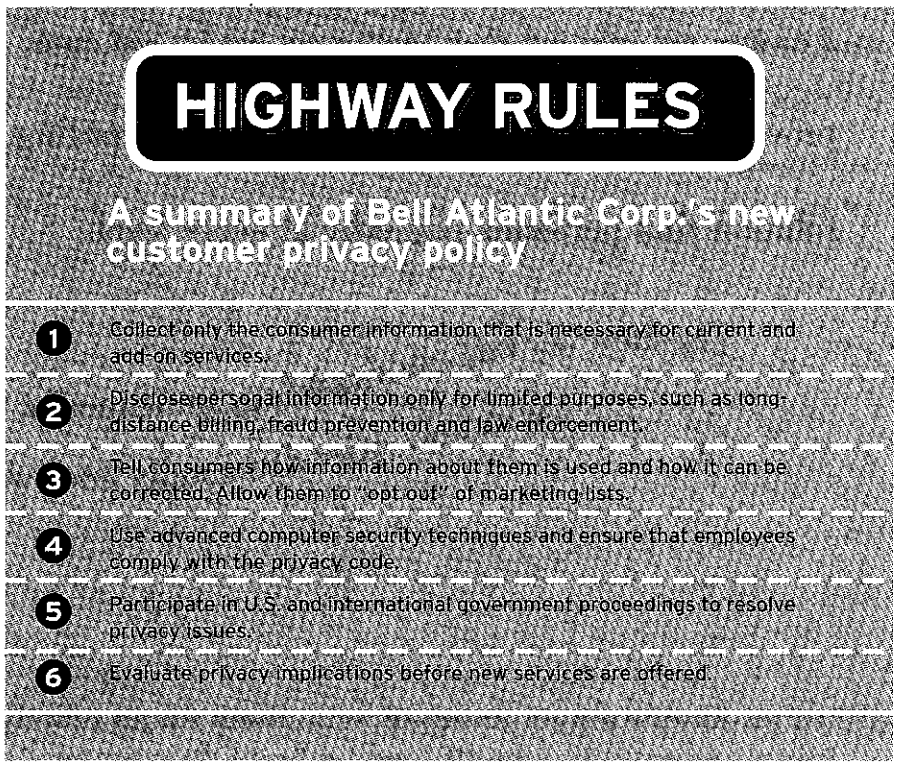
The survey found that, so far, consumers are willing to let vendors self-regulate their behavior. "But the American public has a short fuse on this," Westin warns. Political pressure for a federal privacy board to oversee industry practices and act as a consumer ombudsman is a distinct possibility.

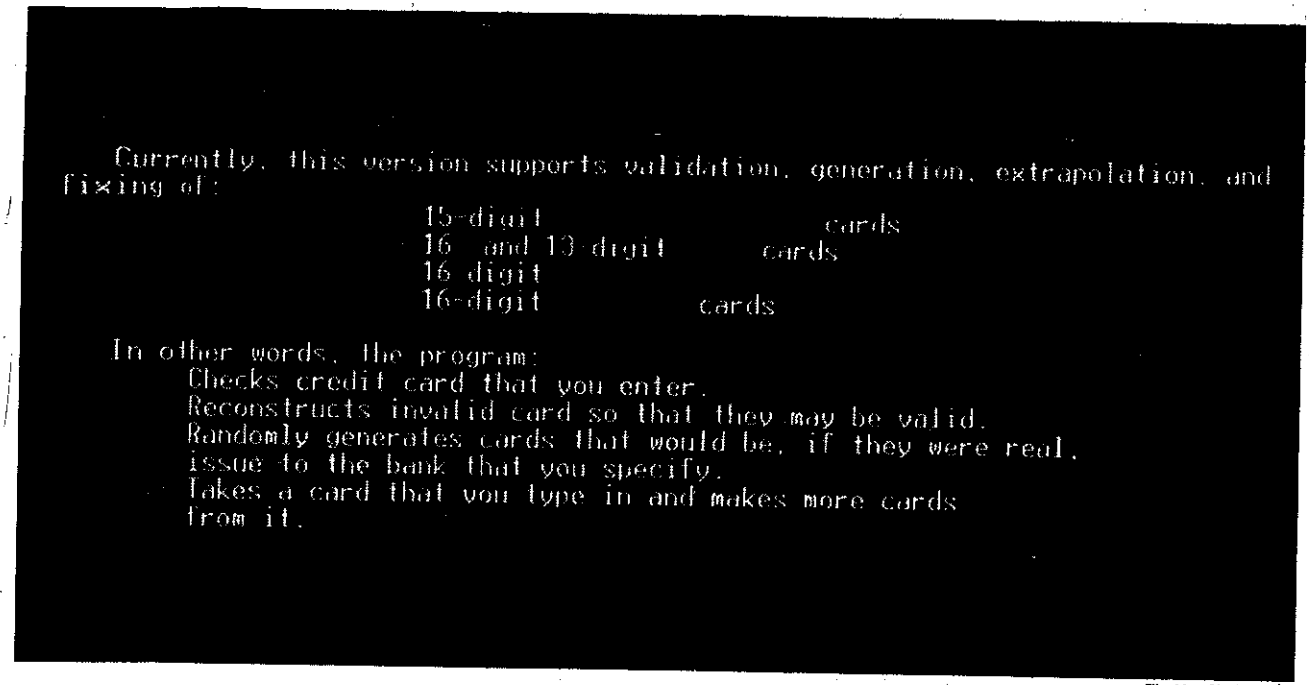
So it is not surprising that information-intensive companies such as American Express Co., Pacific Bell, Equifax, Inc., BankAmerica Corp. and Bell Atlantic have adopted privacy codes to address consumer concerns.

Bell Atlantic's policy was triggered in part by bruising battles with privacy advocates and regulators over the Caller ID service a few years ago. Now the company wants to take a more proactive approach and consider privacy implications *before* it rolls out interactive services, Young explains.

But Young acknowledges that hammering out the privacy code was a "very difficult" process inside ours, and then they scramble to write some privacy rules, according to the book *Managing Privacy* by H. Jeff Smith at Georgetown University.

Of course, having a policy is no panacea. Smith's book points out that many companies have a big gap between their printed policies and their actual practices. Experts warn that business pressures, untrained employees and lax oversight can all lead to privacy abuses — and it will only take a few highly publicized horror stories to make an already-cynical public leery of driving the information superhighway.✦





The New York Times

Computer users have taken advantage of a program known as the Credit Master to try to generate valid credit card numbers. Credit card companies say they know of no significant losses as the result of the program.

3/19/95

A Pirate Program Creates Credit Cards

By ASHLEY DUNN

It's every bank's headache: a criminal running loose with a fake credit card number. But imagine if anyone could create numbers that would pass initial scrutiny — and then churn them out by the thousands.

Over the last year, an obscure computer program designed to create card numbers has begun circulating on major on-line computer services, like America Online, and the myriad electronic bulletin boards around the country.

Known as the Credit Master, the program — possibly one of several such programs — relies on a little-known truth about credit cards: their numbers are not all randomly generated; rather, the card numbers start with a standardized bank code, followed by a coded final digit that can be determined through a simple mathematical formula.

The codes and formulas are not exactly a secret, although banks do not generally like to talk about them. Criminals have long fiddled with the technique of generating such numbers, even though credit card officials, who first began noticing the program late last year, say it invites only the crudest methods of fraud.

Only 3 to 5 percent of the numbers the program generates actually correspond to active accounts with enough credit to make purchases. Moreover, the program cannot tell the expiration date, holder's name or other information related to a card, which are often checked before spending is authorized.

But because there are more and more ways to charge services by typing numbers into computers or touch-tone phones, the program could help enable large-scale, trial-and-error automated sprees, in which hundreds of potentially valid card numbers were tested to find a handful that work. Like "blue boxes" in the 1960's, which allowed anyone with a soldering iron to make free phone calls around the world, the card-generating program of the 1990's has become a vehicle to spread introductory high-tech crime to the masses.

Credit-card companies say they know of no significant losses as the result of Credit Master. And for many of those who have retrieved the program, crime has little to do with their interest.

The program is one in a long line of minor underground

Continued on Page 44

...Verona Park in Verona, N.J. Today's high should near 50 degrees, with some clouds

Pirate Computer Program, Crude Counterfeit Credit Cards

d From Page 37

have been embraced
not for their potential
l tools, but for the
npse they offer into
worlds of telephone
companies.
to have," said a 15-
ersey youth who did
urther identified for
into trouble. "Most
program, but aren't

s authors of the pro-
emselves Micropir-
on its program's
that "the possibili-

want to check a
one," or "make
the blue or even
out of an old one,
do the work," they
oo good to be real.
"
erator programs
han simple calcu-
e a collection of
formulas to cre-
digits.

"A high school student could write this program," said Mark Seiden, a computer network-security consultant in California. "A high school student probably did write the program."

Of the 13 to 16 digits on a credit card, the first group of numbers are bank codes. The digits that follow are largely random, except for the last one, which is known in industry jargon as a "checksum." That number is the result of a mathematical equation using all the preceding digits.

It was created not as a security measure, but as a way to prevent typographical errors. Through it, a clerk entering a number on a computer terminal could immediately tell if a digit did not fit with the rest of the numbers on the card.

The only thing that Credit Master and similar programs do is generate credit card numbers with the correct checksum. The program is legal because it uses publicly available information.

"We consider it a threat, but the formula was never meant to be high-tech security screening," said Dennis Fiene, director of fraud control for Visa.

Of course, there are many other ways to get valid card numbers, like rummaging through a garbage can or looking over someone's shoulder.

The numbers produced through the Credit Master program can be used only for purchases through phone or computer lines, because there is no card to show a merchant.

One of the biggest deterrents to using the program is the ease with which investigators can arrest card hackers if they try to buy anything and then have it delivered.

The police can stake out the addresses to which merchandise is being shipped and arrest the suspects when they arrive — which is how the Nassau County police last week arrested four college students who created their bogus numbers through a variety of techniques and went on a yearlong, $100,000 buying spree. It is unclear what program the students used.

Overall fraud is down at most credit-card companies in the last two years, after doubling from 1988 to 1992, as defensive tactics grew more sophisticated. The companies can now electronically verify for merchants the shipping and billin addresses of a card holder. For pur chases made in person, there ar new numbers encoded onto credi cards' magnetic stripes that canno be easily forged.

And over the next five years, Mastercard and Visa are hoping to introduce another line of defense, replacing the magnetic stripes with computer chips.

The Micropirates, who are only known through their computer nicknames — like Pyro Beast, Xenocide and Rudolph the Red — say that one of the more popular uses for the cards is getting free time on computer networks like X-rated computer bulletin boards, which generally don't make a thorough check of a card number until later.

But even there, access might not be as easy as prospective thieves might be led to believe. Some such companies immediately verify card numbers, and when they uncover fraud, deny access.

Washington Talk: How Government Works