HOW JON HUNTSMAN SWINGS GIANT DEALS WITHOUT CASH

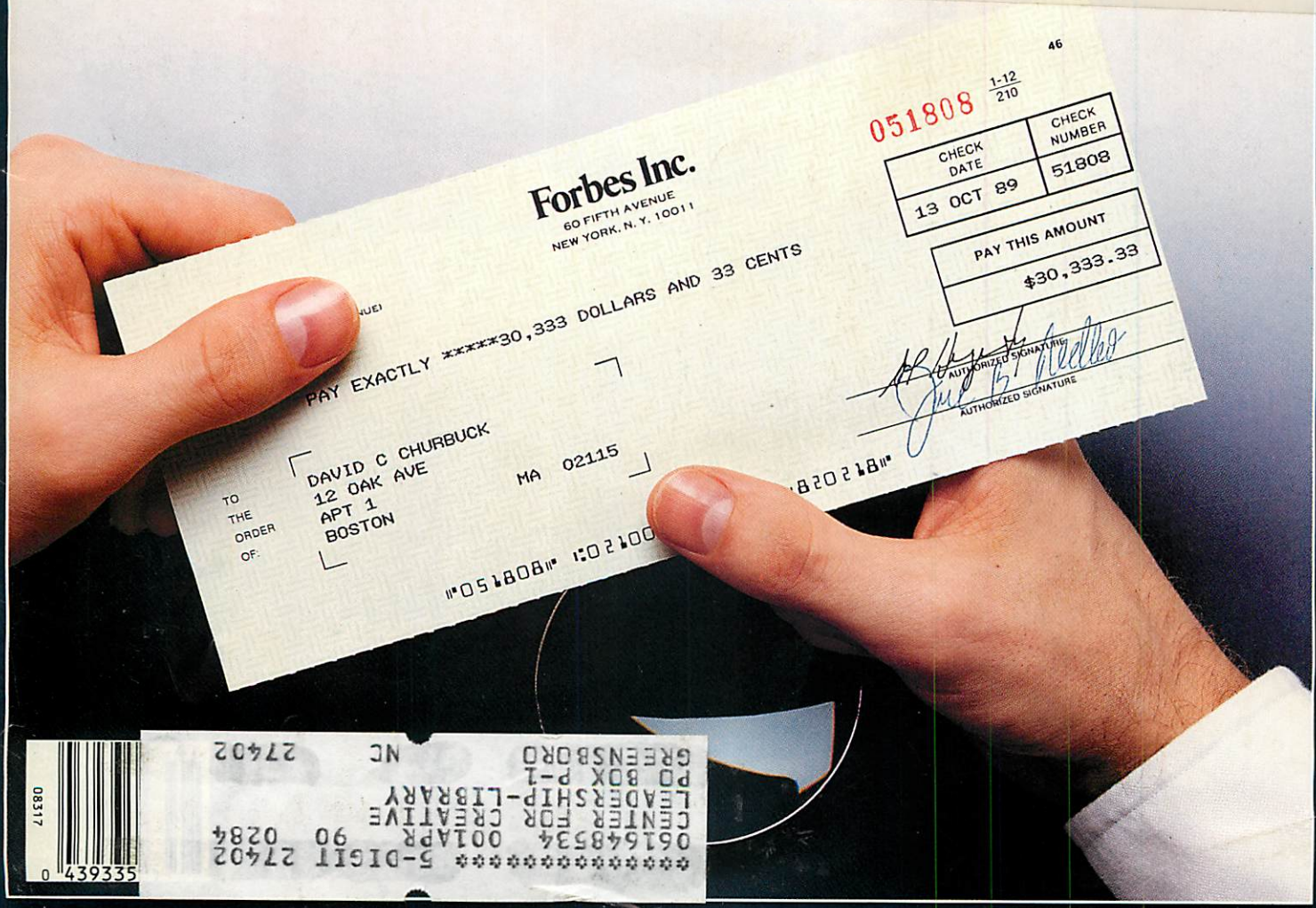
RUPERT MURDOCH ON THE ARROGANCE OF THE CULTURE ELITE

NOVEMBER 27, 1989 THREE DOLLARS SEVENTY-FIVE CENTS

Forbes

THIS CHECK IS A FAKE

Computers are user-friendly for crooks, too. Are bankers prepared? Apparently not.



08317
0 439335

The personal computer is a handy tool for businesses trying to cut their printing bills. It is also a dream come true for crooks.

Desktop forgery

By David Churbuck

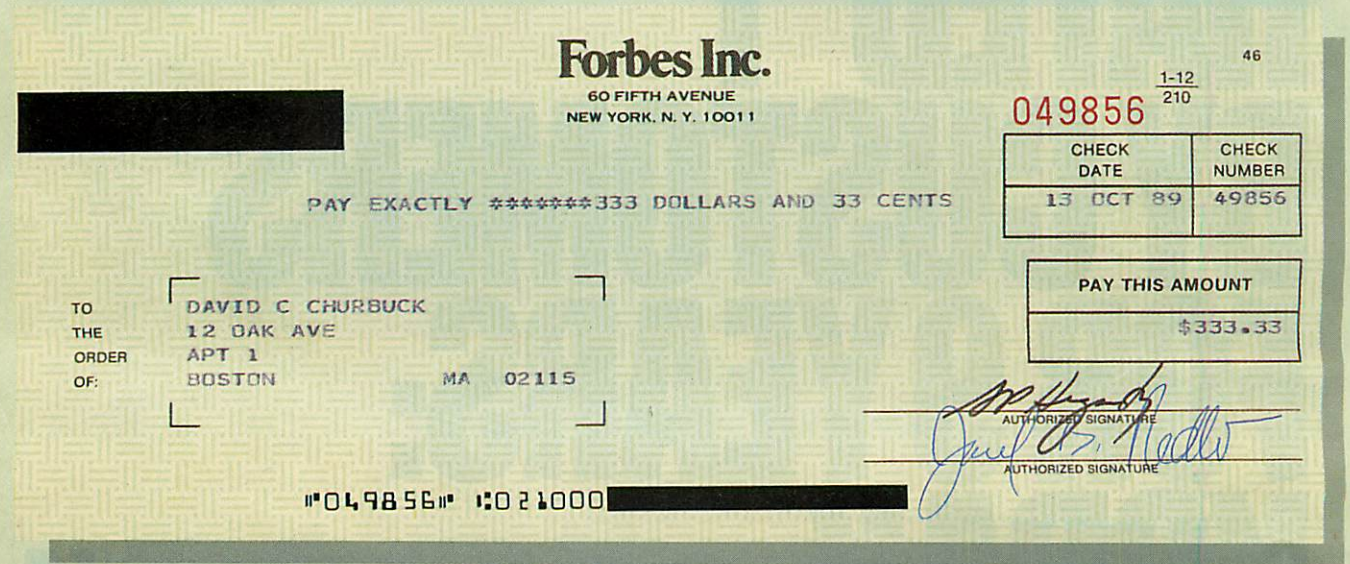
Paul Sjiem-Fat, a Netherlands Antilles national living in Boston's North Station neighborhood, claimed on a Bank of Boston credit card application to be an employee of the Dutch consulate. After he defrauded the bank of about $20,000, the bank discovered that his employment claim was a lie, and, since it involved impersonation of a diplomat, the Secret Service was called in, a search warrant was issued and Sjiem-Fat's apartment was raided.

Investigating this seemingly routine case, the Secret Service stumbled upon its first-ever case of computer forgery. It is certainly not going to be the last. While crooks are only just beginning to learn the game, the possibilities are nearly endless: letters of credit, job recommendations, property records, insurance claims, expense account receipts, college transcripts, business licenses. In short, many of the paper credentials on which society relies are henceforward suspect.

What made this Boston case especially alarming was that Sjiem-Fat used no sophisticated equipment. In his apartment police found a personal computer, a laser printer and nine bogus checks totaling $146,500. In a highly original—and perhaps pioneering—way, Sjiem-Fat was using ordinary desktop publishing tools as instruments of crime.

Here is what he apparently did. With the sort of desktop publishing equipment you can buy at any computer retailer, Sjiem-Fat convincingly forged Digital Equipment Corp. letterheads with a phony name, Paul Marques, and a phony vice president title. He also created phony cashier's checks from banks like First American and Chase Manhattan. Stewart Henry, an investigator with the U.S. Secret Service, explains: "He used the official emblems from three different banks and transferred them onto blank check paper with a laser printer. This was the first time we had ever seen anything like this."

According to investigators, Sjiem-Fat used bogus checks to buy computers from various Boston suppliers. After taking delivery of the computers, he sold them for cash to buyers in the


Forbes Inc.
60 FIFTH AVENUE
NEW YORK, N. Y. 10011

46

049856 1-12/210

CHECK DATE	CHECK NUMBER
13 OCT 89	49856

PAY EXACTLY *******333 DOLLARS AND 33 CENTS

PAY THIS AMOUNT
$333.33

TO THE ORDER OF:
DAVID C CHURBUCK
12 OAK AVE
APT 1
BOSTON MA 02115

AUTHORIZED SIGNATURE

AUTHORIZED SIGNATURE

⑈049856⑈ ⑆021000

Real Forbes expense check, with certain vital elements obscured
A crook would start with something like this.

Caribbean area.

An isolated case? Not necessarily. Just last month a rash of computer-generated fake checks hit the Phoenix area. "These look like they were done by putting corporate logos onto check paper with a desktop publishing system," says Gail Thackery, an assistant attorney general for Arizona.

Coupled to a good printer and the right software, the personal computer is a powerful publishing device. It can create and store logos as well as type in all sizes and styles. With a scanner, it can read in a document, then modify and reprint it. It is, above all, quite accessible to the amateur. Now you can produce professional-looking brochures and blank business forms without hiring a master printer. You can also, if your taste runs that way, run off a bogus check or two.

The existence of all these potential counterfeiting tools is scary enough, but an unrelated development threatens to turn the situation into a disaster for the banking industry. This other problem is a federal statute compelling banks to give their customers quick access to funds from deposited checks.

The quick-access rule was heralded as a victory for consumers. But it was an even bigger victory for con artists. Why? Today's forger can make crisp and convincing business checks, deposit them into an account opened previously under a fake name, demand cash after waiting as little as three days, and be out of town long before the forgeries are discovered. If the forger has chosen as target a corporation with a large balance and a lot of check volume, it's next to impossible for either the bank or the corporation to detect the scheme without doing a monthly statement reconciliation. And that reconciliation can't possibly take place within three days of when a bogus check is deposited.

In the past, a forger had to have access to professional printing equipment and presses. He either owned a print shop, bribed someone who worked at one, or made do with whatever materials he could copy by hand. The risk of detection was high. Not any longer. The boom in desktop publishing has brought a flood of typesetting products to market, at declining prices and increasing capabilities.

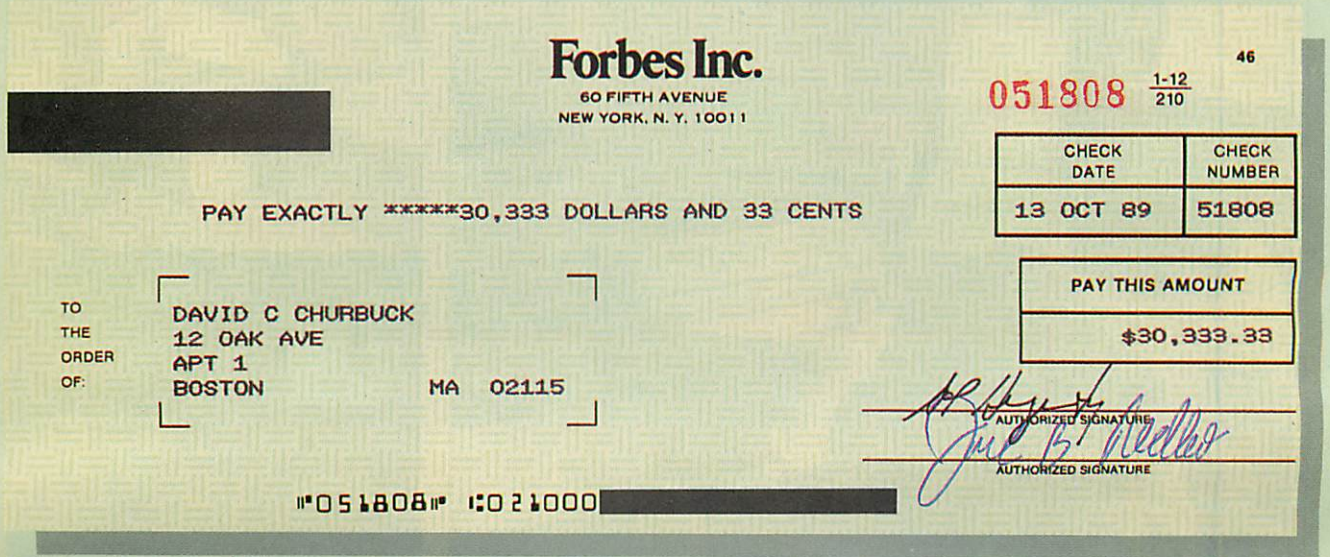
"The market for this equipment has gone wild in the last year," says James Cavuoto, a Torrance, Calif. desktop publishing expert. "It's only a matter of time before the crooks catch on to the opportunity." They clearly already have.

How much computerized forgery goes on? A few years ago, next to none did; the equipment was expensive and inadequate. Now, probably a fair amount, although the authorities have yet to classify PC forgery as a crime separate from conventional forgery, and have no statistics on it whatever. (The Boston case, which sent Sjiem-Fat to a federal prison in September, is one of the few that have come before a court.) Total forgery, fraud and embezzlement losses at banks and other financial institutions ran $860 million in the U.S. last year.

In a few years, however, the computer forgery problem could explode. Equipment is getting cheaper and higher in resolution every day. The first laser printer cost $200,000. The current Apple NT desktop printer costs only $3,900—and has the same 300 dots per inch of resolution. Steven Jobs' new Next system promises a printer with 400-dot resolution. Scanners vintage mid-1970s cost $100,000 and could do black and white at a detail level of 300 dots per inch. Today's crop can do color scanning at 600 dots and cost about $10,000, while black-and-white scanners cost under $1,000.

What can the bad guys forge on a computer? Almost any printed document that has neither color nor texture in it. Particularly easy are plain-paper documents passed in situations where scrutiny is low. A band of shoplifters in the Philadelphia area used crude computer forgeries to dupe stores into acting as their own fences: forge a receipt for expensive clothes like leather coats, return them to customer service and walk off with a refund or check. One executive of a desktop publishing company says his teenage son used the equipment to create a fake ID in order to buy beer.

Forging of bank documents is an intriguing possibility. It may have helped William Stoecker (FORBES, *Oct. 31, 1988*) stiff leading banks out of tens of millions of dollars. Connecticut Bank & Trust has turned over to a bankruptcy court a letter and a note written on its letterhead that purport to release Grabill Corp.'s Stoecker from certain financial restraints. Grabill later filed for protection under Chapter 11; the documents, says CBT, are forged and not produced on the bank's word processing equipment. Stoecker's lawyer flatly denies this, and says he has document experts



Fake FORBES expense check

Once you get the design scanned in, you can write your own ticket.

willing to back him up.

At this date, color is an impediment to computer forgers, since color printers print on waxy paper that is unlike ordinary printing paper. But this situation may change overnight. The newest Canon color copier, the CLC500, prints with superb detail on plain paper, and Canon has plans to add a connector that will enable the machine to be hooked to a computer for the printing of computer-generated images.

If bankers aren't terrified by all this, they should be. Two months ago a con man deposited in a European bank $3 million worth of bogus cashier's checks drawn on the New York branch of a German bank. The checks, which have a distinctive color background, were probably made from fake check stock created with a color copier of Canon quality. Investigators still haven't figured out how the payee and deutsche mark amounts were added, but a computer laser printer is one possibility. The imitations were far from perfect, but they did clear the New York branch. The crook cleaned out the European account soon thereafter. The police are still groping for leads.

Not surprisingly, the new generation of color copiers has the Bureau of Engraving & Printing in a panic. Since 1986 plans have been in place to redesign the currency to include repeated microprinting and special polyester threads. The bill redesign, due in the early 1990s, will probably thwart the color copier crowd.

But what is the banking industry going to do to ward off counterfeit checks? It doesn't have an answer. When Congress passed the quick-release law on deposited checks last year, a few Cassandras raised the issue of fraud losses. But they were drowned out by a chorus of consumerists, who said the banks' prime motive in putting holds on checks was to profit from the float.

"Technology has increased crime—that's a fact of life in this industry," says Boris Melnikoff, vice chairman of the American Banking Association's security and risk management committee. "The new regulation makes a banker's life much harder but makes things much simpler and faster for the thief."

To be sure, the desktop computer did not create the crime of forgery. All it did was make the tools user-friendly. Check-passers can now practice forgery in the privacy of their homes, without enlisting help from crooked

Anatomy of a scam

How easy is it to fabricate a check that looks real? And to pass it through the banking system? Very. Here's how we did it, although some key steps are deliberately omitted. Our purpose, after all, is not to print a manual for crooks. We simply want to make business people aware of what crooks already know. They need some reminding of the risks. Virtually all of the banks contacted by FORBES for this story said they had no special measures in place to detect or prevent computer-assisted forgeries.

Get a real business check to use as a model. Professional scamsters often get refund checks from airlines by paying cash at the ticket counter and then coming up with a reason for not taking the flight. Other possibilities are merchandise refunds and dividend checks. Needless to say, the crook would cover his tracks by having the refund made payable to a false identity.

Why a business account? Because it's likely to have enough money in it that several large forgeries will clear. In one recent case now being investigated by the FBI, a forger intercepted a personal check drawn on one of those tony New York banks that take only wealthy "private banking" customers. He drafted five $30,000 imitations (same account number, different check numbers), all payable to a fictitious firm. He deposited the checks in a California bank, waited a few days for them to clear, then emptied his account. An investigator says that the fakes appear to have been made on a computer.

1

2

printers who might squeal on them someday.

Take a look at the fake FORBES check shown on the cover and on page 247. It is an amateur job, created by a reporter with no previous experience in forgery. The green safety paper and the red numbering stamp came from stationery stores. The black parts of the blank check came out of an Apple NT laser printer attached to an Apple Macintosh personal computer and an Apple scanner. The signatures are hand-drawn imitations, not nearly good enough to fool a handwriting expert but plenty good enough to fool a bank clerk. No, banks by and large do not check signatures before paying on checks.

How about the magnetic ink that encodes the bank routing number and account number at the bottom of a check? Magnetic ink printers were once expensive (circa $400,000) machines available only to banks and legitimate check printing companies. No longer. In 1987 Digital Design, a Jacksonville, Fla. firm, announced its Model 636 laser printer for personal computers. Using magnetic toner, the printer is aimed at the government and banking industry and companies that sort their business forms with magnetic scanners. Price tag: $7,388, excluding software.

The new machine is an open invitation to crooks. An executive at Digital Design insists, "All the corporations we sell to are reputable ones." But since this low-cost machine has legitimate application outside the banking industry, it will be next to impossible to police its use.

Doctored receipts illustrate a different, and indeed much easier, application of desktop publishing. The document doctorer of a decade ago was known as a "pen and ink man," someone wearing a green eyeshade with a lot of patience and a steady hand. Today's has a much easier job. A desktop scanner converts a paper document into a digital file that can be manipulated with keyboard and mouse commands before it is printed again in crisp detail on a laser printer. Gone are bottles of Liquid-Paper, scissors and tape.

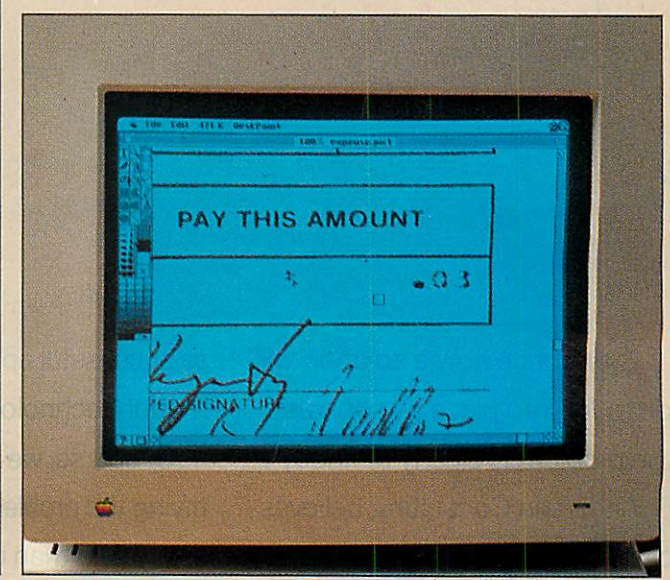
"Laser printers are our newest and biggest challenge," says James Davidson, a document specialist of the Internal Revenue Service's forensic laboratory in Chicago. Why? He switches on an ultraviolet light and shows how easy it is for a trained person to detect a crossed-out figure on a receipt. Cut-and-paste jobs photocopied to hide the evidence can also be easily detected. But laser printers don't leave any more evidence than the fact that they are laser printers. Photocopy the output, attach that to your tax

You need some good equipment. A Macintosh II with 8 megabytes of random access memory will run you about $5,000; a Hewlett-Packard ScanJet scanner, $2,190; an Apple NT LaserWriter, another $3,900 (1).

Now scan the check into a PICT file (a standard graphics format read by many graphics programs) by placing it face down on the glass platen of the scanner (2). Install a copy of DeskJet Paint software (or PixelPaint, or any well-known, powerful graphics software) on your Mac. Open the PICT file. Use graphics commands to magnify the image and clean up the edges of the characters, which may be a little fuzzy (3). Other Paint commands, which allow parts of an image to be captured and moved, are key to this forgery (details omitted). We also used a command to enhance a shading effect in the logo of the bank, which the scanner had blurred. You can't see the bank's name in any of the pictures, but take our word for it, it looks just like the real thing.

Now erase from the PICT file the check number that appears stamped in red in the upper right corner of the check. You also have to be intelligent about how you handle the magnetic-coded version of the number at the bottom edge of the check. We're not going to say exactly

3

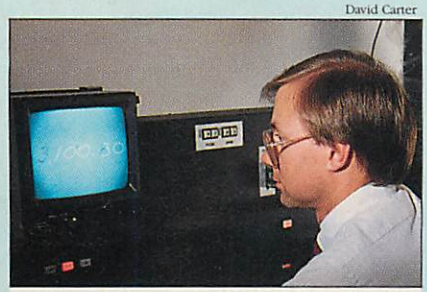


4

Photographs by Rick Friedman/Black Star

Don't mess with tax receipts

David Carter



Detecting cross-outs

In an office building across the street from the Chicago Mercantile Exchange work some of the nation's leading document cops, the staff of the Internal Revenue Service's forensic lab.

Want to fudge your deductions by turning that $300 receipt into an $800 one with the stroke of a ballpoint? Don't risk it. The IRS has ultraviolet scanners, ink chromatographers, densitometers and argon-ion lasers that can identify the brand of pen, the age of the paper and the source of the paper. James Davidson, a document specialist at the lab, explains how people get caught trying to change business receipts: "First of all his pen has to be the right age. We can tell how old the ink in it is. Then he has to have the right paper. You'd be surprised how many people think they can get away with a bottle of Liquid Paper."

But give one of the lab's 31 technicians something printed on a laser printer and the job suddenly becomes much harder. "Laser printers are tough," says Davidson. The lab can tell you that a document was printed on a laser printer, not a photocopier, and who manufactured the paper and when. But it has yet to assemble a set of computer printer samples as exhaustive as its library of paper and ink samples.

"As optics and digital technology improve, we might really start running into a lot of problems," Davidson says. "But technology is what makes this line of work interesting. We can't stand still and rest on our laurels. The cheats would run over us."—**D.C.**

what to do with it.

Copy the image to two other files. Open one copy and delete the payee name, the dollar amount and any other printing or typing or writing done at the time the business cut the refund check (4). Open the other copy and delete everything but these elements.

Load your laser printer with 8½-by-11 sheets of safety paper (5), the kind with a colored pattern that shows rubber erasures. (Ha! Who needs rubber erasers?) Getting this paper is difficult but not impossible. Nor is it illegal; check paper is not a restricted commodity. The safety paper should be a close match to the original. We won't identify our supplier, except to say that he insisted on being paid in cash.

Next, close DeskPaint and open a page layout program such as Quark Express. Format an 8½-by-11 page, open your first PICT file in it and reduce or expand the image until it matches the original check.

Print multiple copies of the check with the laser printer. For first-class work, a separate run through a specialized laser printer is necessary to get the magnetic routing number and check number along the bottom of the check. In that case the check-blank PICT file would be further divided between plain ink and magnetic. We skipped this step in order to save the $7,388 cost of the magnetic-toner printer, but a serious forger would probably want to make the investment.

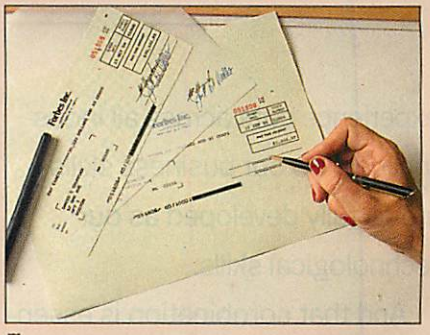
Now open the second PICT file, the one with the payee and amount. If the real check had these elements typed, hook the Mac to a dot-matrix printer with an old ribbon and run the laser-printed blanks through this printer. Alternatively, create payee and dollar amount fields in a word processing program, and find a dot-matrix typeface that matches the typing on the original check. For our test forgery we were attempting to imitate an IBM minicomputer printer, and we used an ink-jet printer on a bold setting (6). It's not a perfect match, but it fooled the bank. Had we been serious, we would have found a typeface that more closely matched the IBM typeface.

Feed the blank checks into the dot-matrix or other printer, carefully aligning the boxes by trial and error. Print the payee name and amount onto the laser-produced blanks.

Now forge the signature(s) with hand-held ballpoint or other pens (7).

5

6



7

return and the best document examiner can't say whether a computer has been used to alter or print it.

"The big problem with computer-generated print is it offers us none of the clues of a typewriter: the irregularities in type, differences in impact," says Jeffrey Luber, chief document examiner with the Suffolk County Criminalistics Laboratory on Long Island. "The difference between one laser-printed document and another is minute."

Publishing consultant Cavuoto says the best way to tell if a document has been printed by a laser printer is to make a sharp fold over some of the type and scrape the edge. If some of the ink flakes off, then chances are good that it isn't ink but toner.

Cavuoto's is a useful hint, but it is, of course, useless if the legitimate receipt or voucher that the crook is altering is itself the output of a laser printer. To save money, businesses are shifting from offset-printed forms stored in filing cabinets to electronic forms stored digitally for laser printing. In so doing, they are making it impossible for auditors or investigators to tell real forms from fake ones.

What can businesses do to protect themselves from computer counterfeits? It's like burglarproofing your car. Nothing will stop a really determined thief, but you can at least make him want to select another victim. "Try to make a document such that someone tempted to tamper with it will be discouraged by some feature or features," advises Thomas Gazda, a document security specialist at Arthur D. Little, the Cambridge, Mass. think tank. "You hope the forger gives up completely and decides tampering isn't their bag, or just moves on to somebody else's document."

One defensive move is to put color on important documents, such as checks and purchase orders. Color is harder to reproduce than black and white. Another, for businesses with a large enough printing volume to justify it, is to order nonstandard safety paper, and restrict your supplier's right to sell that pattern elsewhere.

Other safeguards include: Look for perforations on at least one side of the check. Hold up the check to a light and see if the routing numbers reflect light; if they do, then chances are they weren't printed with magnetic ink.

The check counterfeiter relies on the fact that the money he's going to steal is coming from a checking account with a very large balance. Also, he must have an original to work

There is a clever way to do this that we will not describe here but that is known to every forger.

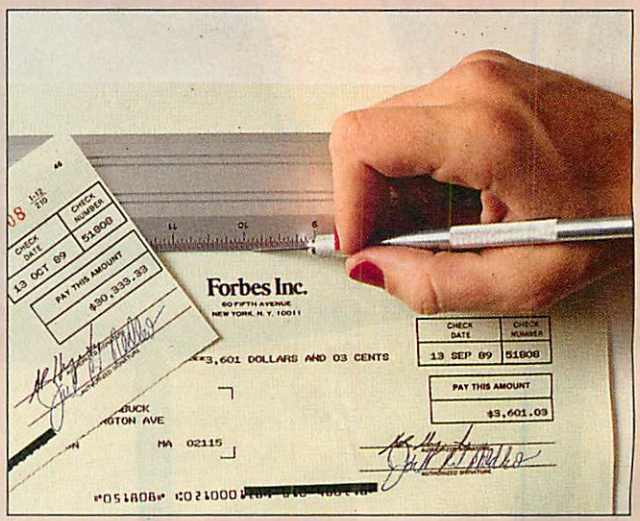
Some checks are numbered in red ink. That's why you deleted the check number in step 4. Go to an office supply store and buy an automatic numbering machine for $50. Ink it up, practice a few times, then stamp the check (8).

Cut the checks with a razor on some sides and a perforating device on the others, according to the pattern of the original (9). Paper perforators are available at office suppliers, but if you can't find a good match create your own perforations with an X-Acto knife.

Deposit the bogus checks in an account, and take advantage of the liberal federal rules on availability of deposited funds. If the routing numbers are accurate, the check will almost certainly clear. Indeed, a test forgery of ours did, even without magnetic toner in the routing numbers. Why? When a check can't be read in a magnetic reader, it is sent to a typist who retypes the numbers and affixes a corrective magnetic strip to the bottom of the check. Thousands of these corrected checks go through the check clearinghouses every night. No one gives them a second thought.

The main story suggests several protective moves for banks and their corporate customers. And if these and similar measures prove inadequate to stop the crooks? We'd hate to stir up a hornet's nest of consumerists, but it just may be necessary to rethink that regulation giving depositors rapid access to their funds.—**D.C.**

8



9

from. Thus, if your business involves occasionally handing out small refund or payment checks to strangers, move those payments through a checking account with a very small balance. Keep a separate account for larger payments to known and trusted vendors. If the crook uses a refund check as the template for printing an $18,000 fake, he may overdraw the account, triggering an inquiry that may just come in time to catch him.

Bank customers have less immediate reason to fear check counterfeiting than the banks do. Absent some real negligence by the bank customer (such as not doing reconciliations promptly), the loser on a forgery is the bank that accepts it as a deposit. But in the final analysis the losers will be the customers. Forgery losses will inevitably be passed along in the form of higher fees or lower interest rates paid. And if you were put out by all the cross-examining you got last time you walked into a bank to open a new account, brace yourself. Next time it will be a lot worse. ■

Buying a computer system from one company has drawbacks. But at least you know whom to blame if the system fails.

Is there a doctor in the house?

By Julie Pitta

NOT LONG AGO, one-stop shopping was the philosophy of the conservative computer buyer. You'd buy your mainframe, storage disks, printers, video display terminals and software from one vendor—IBM if you were really conservative, or perhaps Burroughs or NCR or one of the others. The drawback of being locked into one supplier: high prices. The advantage: knowing whom to blame if the system crashed.

There are still some who cling to the old maxim "No one was ever fired for buying IBM," but they are fewer in number. The proliferation of computer companies and the trend toward "open" hardware and software have allowed customers to mix and match vendors. A large corporation might have a network of personal computers from Compaq Computer Corp. and Apple Computer Inc., engineering workstations from Sun Microsystems

Gerry Mooney