

Counterfeit Identification

**A manual for the Identification of
Counterfeit Currency, Credit Cards,
Traveler's Cheques and Bank Checks**

**By: L. Burke Files
lbfiles@feeinc.com**

Table of Contents

Identification Reference Sheets	3
Credit Cards	3
Traveler's Cheques	5
Bank Checks	9
US Currency	10
Issuer Contacts	11
Stories from the Field	12
Glossary of Terms	29

Identification Reference Sheet for Credit Cards, Travelers Checks, Bank Checks and Currency

Note: Only the issuer can determine if an item is genuine or counterfeit. This reference sheet is to help identify items that may be suspect.

Credit Cards

American Express

- Description: American Express issues four credit cards: the Personal Card, the Gold Card, the Platinum Card, and the Corporate Card. In March 1987, American Express instituted the Optima Card, designed to be a companion card to existing Personal, Gold, and Platinum cards, and issued only to card members in good standing for one year. Card numbers are the same as for other American Express cards; background is blue with gray engraving of centurion, which may be on the left or the right side. Border and card title are white.
- Numbers: The account number is 15 digits, beginning with 37 or 34, and is sequenced 4-6-5.
- UV Light: There are large letters reading "AMEX" and phosphorescence in center portrait will be visible.
- Microprinting: There is microprinting along the bottom of the front of each card.
- Other: Beginning and expiration dates appear above cardholder's name.

Diners Club/Carte Blanche

- Description: Basic Diners Club card has silver and blue logo at upper left, Citicorp logo below; silver background with faint wavy lines. "Business Card," "Corporate Card" may be at right. Photocard: border color varies, may omit border. Partnership logo may appear in place of member signature, or be on card back, bottom right. Carte Blanche has blue logo; white background, gold edging.
- Numbers: Both cards: 14 digits sequenced 4-6-4.

Discover Card

- Description:** The Discover card has a black background, overprint of Discover repeats across data area; green and white Novus logo is at bottom right. Also valid until Sept. 1996; Discover card with gray overprint of Sears Financial Network. On both cards, there is a sunset photo backdrop across Discover heading, sunburst in middle of the "O." The Discover Private Issue card has a black background, overprint of Private Issue (in script) across data area, and green and white Novus logo at bottom right. Also valid until Sept. 1996; similar card with overprint of Sears Financial Network, with Novus logo, taller Discover heading.
- Numbers:** All cards have 16 digits, sequenced 4-4-4-4. The first four digits are always "6011."

MasterCard

- Description:** Standard MasterCards may be on plain stock or graphic. There are three valid MasterCard card holograms. Each appears on the right-hand side of the card; note that the MasterCard logo of interlocking red and yellow circles with the word MasterCard in white letters may appear above or below the hologram on all newly designed cards.
- Numbers:** Embossed account number has 16 digits sequenced 4-4-4-4. A repetitive MasterCard design appears on the signature panel of the card.
- UV Light:** Under Ultraviolet lights a "M C" will appear on the bottom half of the card.
- Other:** Some card issuers have elected to use a MasterCard with a unique security character embossed on the face of the card to the right of the valid dates. The interlocking M and C. If the security character appears, the signature panel on the back of the card will contain an indent printed account number followed by a 3-digit validation code. In addition to the standard card, a (silver) MasterCard BusinessCard is issued, as well as a Gold MasterCard.

VISA International

- Description:** All VISA cards should have either a panel at the right with a hologram of the VISA dove or an area that contains both a hologram of the dove and the VISA logo above or below. Remainder of the card will have varying designs selected by the issuing financial institution.
- Numbers:** Cards may have either 13-digit or 16-digit account numbers; the first digit is always 4, sequenced 4-3-3-3 or 4-4-4-4. Four-digit number printed above or

below embossed account number must match first four digits embossed below. This is the BIN number. Signature panel on the back should bear repeat of "VISA" in blue and or orange at a 45 degree angle.

- UV Light:** Under ultraviolet light a dove, similar to the hologram, will appear in the center of the card.
- Microprinting:** Around the Visa logo on the bottom right of the card microprinting with the BIN number repeated should appear.
- Other:** There is a special "V" at the end of the expiration date. "CV" on classic cards, "PV" on premier and gold-colored cards, and "BV" on business cards. Effective 1/1/96 "C," "P," and "B" will no longer be required and will eventually disappear.

Travelers Cheques

American Express

- Denominations:** U.S. \$20, \$50, \$100, \$1,000 (\$10 T/Cs are no longer being produced but many are still in circulation). Besides U.S. Dollars, T/Cs are produced in Australian Dollars, Deutsche Marks, Dutch Guilders, Swiss Francs, French Francs, Pound Sterling, Canadian Dollars, Japanese Yen, Saudi Riyals (payable only in Saudi Arabia), ECU (European Currency Unit) is no longer produced but may be in circulation. American Express Travelers Cheques are valid without time limit; therefore, cheques of earlier issue and design may continue to be presented for payment indefinitely.
- Paper:** Special watermarked paper when viewed show "AM EX CO" with a globe.
- Background:** There are four types of the American Express Travelers Cheque: (1) Traditional: Wavy purple pattern, "AMERICAN EXPRESS" is repeated across the top portion of the cheque above the city/date line. The centurion is located on the left side encircled in an oval frame. (2) New Design: Blue diagonal wavy lines are above the top left-hand signature line. A new larger centurion portrait is located on the left side of the cheque. Several other anti-counterfeiting features have also been added to this design, one of which is a see-through register on the globe located on the face and reverse of the cheque. (3) Gift Cheque: Printed on gold paper with a mauve/aqua pattern and produced in U.S. dollars in the amounts of \$10, \$25, \$50, \$100. "AMERICAN EXPRESS" in 1/4" high gold letters appears at the top in a lozenge with background colors that graduate from aqua to mauve to aqua.

The central background features an acanthus scroll pattern. The Gift Cheque will soon be revised to look similar to the newly designed cheque. (4) Cheques for Two: Are produced only in \$20, \$50, \$100 U.S. Dollars and are almost identical to the traditional and new design. The only exception is that 2 signature lines appear in the upper left-hand corner. The words "signature 1" and "signature 2" appear over the signature lines.

- Engraving:** "American Express Travelers Cheque" and all other wording and borders on the front of the cheque feature raised dark navy blue ink. The Gift Cheque border, portrait at left, and text feature raised black ink.
- UV Light:** Under ultraviolet light both of the signature blocks will be highlighted and the blue security seal will be highlighted.
- Microprinting** Both the denomination button on the front center right and the counter signature line contain microprinting.
- Other:** Unit of currency appears at the top of each cheque. The currency and denomination appear on the bottom of the cheque. American Express has added several denomination buttons to the newly designed cheque. The denomination mark on the left rear of all cheques will smear when wet. The right denomination mark will not smear.

Bank of America

- Denominations:** U.S. \$20, 50, 100, 500 1,000. (Earlier format, issued until 1982, had a U.S. \$10 denomination.) Also Deutsche Marks, Pound Sterling. Cheques are colored-coded according to currency.
- Paper:** White, but with no border showing. A triple globe watermark appears on the left side of the cheque.
- Background:** A repeated swirl design fades from blue on the sides to gold in the center, with a large repetitive motif of BA and the cheque's denomination.
- Engraving:** Bank America heading is engraved in dark blue with words "Travelers Cheque" in phantom letters. Dark blue denomination is engraved at right superimposed on blue and red spiral design. 1/8" multicolored (blue/red) band is engraved at bottom of cheque.
- Other:** Triple globe symbol on the face of the cheque is printed in blue and gold. Back of cheque has red and blue map projection motif. Countersignature line is vertical at left-hand side of cheque. Earlier issues (still valued) differed in printing style.

Citicorp

- Denominations:** U.S. \$20, 50, 100, 500, 1,000 (U.S. \$10 denomination issued until 1988: still valued)
- Paper:** White paper with shaded watermark of Mercury on the right-hand side of the cheque.
- Background:** Repetitive "Citicorp" printing fades from gray to green to gray across the face of the cheque.
- Engraving:** Since 1988 border and text are engraved entirely in black ink. On cheques manufactured through 1987, the border and text are engraved in black ink. The black ink on the sides fades to green ink in the center. These cheques are still acceptable. A full-figure reproduction of Mercury is engraved on the left side of the cheque.
- Other:** Uniform gray swirl design appears at right in location of watermark. A star on the back will appear in the center of the orange star on the front when the cheque is held up to the light. A "Private Brand Version" can have the seller's name printed above the word "Citicorp" and the seller's logo to either right or left.
- Note:** On earlier issues, Mercury figure was smaller. Border and text were printed in black; background in green. Heading in center of top border reads: "First National City Bank" below. Either an ornate compass or a Private Brand Insignia appeared at the right. These cheques have not been printed since 1976, but they are still valued.

MasterCard

- Denominations:** U.S. \$20, 50, 100, 500, 1,000 Also other world currencies.
- Paper:** White paper is embedded with fluorescent fibers that are visible under ultraviolet light. Goddess watermark is visible from back side of cheque through the white globe area on the left-hand side.
- Background:** Repetitive pattern reading "MasterCard" with the denomination (e.g., MasterCard 50 U.S. Dollars) is printed in pastel purple, blue and white, using special inks that will blur if erasure is attempted. A multicolor (olive green/pink) spiral design runs across the center face of the cheque from side to side.
- Engraving:** Border and text are engraved; border in dark blue, purple and brown, text in dark blue. Latent images engraved on either side of the heading read "M" and "C" sideways when the cheque is held flat at eye level. Round engraving at

left has either a goddess, etc. (Cheque) logo, or other symbol. Right-hand engraved area has denomination or portrait of Thomas Cook.

Other: Red and yellow globes and MasterCard logo are printed with fluorescent ink that is visible under ultraviolet light. The outline of the MasterCard symbol on the back of the cheque is in perfect register with the one on the face of the cheque. Cheques may be personalized by an issuing institution above the countersignature line; the name, location and authorizing signature of the issuer will appear at the lower right. Older format has different background pattern and colors, latent MC image at right instead of on top, and a larger globe logo. These cheques are still valid.

Republic

Denominations: U.S. \$10, 20, 50, 100

Paper: White paper with multicolored-colored fiber discs embedded.

Background: Printed with several alternating pastel shades of blue, purple and brown. The words "REPUBLIC NATIONAL BANK OF DALLAS" repeated, swirl around the bank seal which is centered in the bottom half of the cheque. Seal has a blue and white star in the center.

Engraving: Border and text are engraved in dark blue ink. Headings are white in blue engraved fields. An allegorical head is engraved at the left; amount of cheque, superimposed on large dollar sign (\$) is engraved at right.

Other: There have been five issues of National Travelers cheques. They may vary slightly but all are still valid. Two early issues did not include magnetic coding field at the bottom left.

Note: Republic no longer issues traveler's cheques as of April 1986, but all previously issued cheques are still valid.

VISA

Denominations: U.S. \$10 (no longer issued, but may be negotiated), 20, 50, 100, 500, 1,000
Also Deutsche Mark, Swiss Franc (no longer issued, but may be negotiated), French Franc, Pound Sterling, Canadian Dollar, Spanish Peseta, Japanese Yen and other major world currencies.

Paper: White paper has been watermarked with a globe and a dove on either side of the VISA card symbol.

Background: On the right, light blue fades into pink; on the left, bands of gold and white radiate from central VISA card symbol. The word VISA and the

denomination of the cheque are repeated in small white letters (or gray on the white band portion of the cheque) across the face of the cheque, e.g., "VISA US 50 VISA US 50". Cheques issued before 1982, no denomination is found only the word VISA is repeated throughout. Cheques printed after 1987, a large- denomination numeral is located above the VISA mark on the face of the cheque. On the reverse side, denomination numerals appear in the upper and lower bands.

Engraving: Border and text are engraved in dark blue ink; a portrait of a dove is engraved at the left; the primary denomination indicator is engraved at the right. The words "TRAVELERS CHEQUE" are engraved in the gold band of the VISA card symbol.

Other: Cheques are printed with security inks that will reveal erasure attempts. The name of the issuing institution will appear to the right of the VISA card symbol and may be printed in the upper left-hand corner of the cheque.

Bank Checks

General: Bank Checks are non-standard and one can find on the checks everything from detailed security features to cartoon characters. One must be familiar with the banks in their area, the Federal Reserve numbering and routing codes common to their area.

Features: Look for a padlock on the front of a check. When you see a padlock on the front a listing of the security features will be printed on the back in a light security screen. Read those features and compare those features with the check, the MICR printing on the bottom of a check is difficult to duplicate correctly. Use either a MICR check viewer or a MICR reader on these numbers. If they are placed incorrectly and or do not read in the MICR reader it is likely that there is a problem with the check. View the check under a magnifying glass and look at the printing. If the ink is embedded in the paper, usually in little dots, it is probably a good check. If the colors are uniform it probably was printed on an offset press and if they appear three dimensional it was probably copied.

U.S. Currency

Past to 1990: In general U.S. Currency should have the feel of money, have raised intaglio type printing and have magnetic properties to the ink in certain places, but only on the front of the bill. The paper will be of a high quality fibrous nature when viewed with a magnifying glass and will have small red and blue fibers imbedded within the paper. The over printing of the black ink on the green of the Treasury seal should be clear and clean. The portrait should look clean, not muddy or blurred. The background of the portrait should consist of fine line detail and not be a solid color. There are 12 Federal Reserve "Branch" offices and they have a letter assigned to them from A to L, the first through 12th letter of the alphabet. In the four corners of the bill there will be a number that corresponds to the letter of the alphabet, 1-12.

Series 1990: Excluding singles, the 1990 and forward series of bills have a plastic denomination fiber placed in the left side of the bill. When held up to the light this fiber will show the denomination of the bill. Around the outside of the portrait you will find the words "THE UNITED STATES OF AMERICA" repeated in microprinting.

Series 1996

100's The portrait of Franklin has been enlarged and placed off center. In Franklin's lapel you will find in microprinting the words "THE UNITED STATES OF AMERICA". Around Franklin's head the background of the portrait has concentric lines following the outline of the portrait. On the left you will find a redesigned Federal Reserve Seal and a denomination fiber that will glow red/orange in color under UV light. The lower right denomination button contains microprinting repeating "USA100". When held up to the light you will see both the denomination fiber on the left and a watermark portrait of Franklin on the right.

50's The portrait of Grant has been enlarged and placed off center. In Grant's shirt lapel you will find in microprinting the words "THE UNITED STATES OF AMERICA". Around Grant's head the background of the portrait has concentric lines following the outline of the portrait. On the left

you will find a redesigned Federal Reserve Seal. On the right and a denomination fiber that will glow yellow in color under UV light. When held up to the light you will see both the denomination fiber on the right and a watermark portrait of Grant on the right.

20's The portrait of Jackson has been enlarged and placed off center. Under Jackson's portrait and on either side of his name you will find in microprinting the words "THE UNITED STATES OF AMERICA". Around Jackson's head the background of the portrait has concentric lines following the outline of the portrait. On the left you will find a redesigned Federal Reserve Seal. On the far left you will find a denomination fiber that will glow green in color under UV light. When held up to the light you will see both the denomination fiber on the left and a watermark portrait of Jackson on the right.

10' and 5's These different denominations have begun printing and will be pleased into circulation in early to mid 2000

The lower right denomination button is embossed for a raised feel and has color shifting ink. When held from different angles it will look either green or black. Under magnification it will appear to look like iridescent green and black glitter, not like ink at all. When held up to the light you will see both the denomination fiber on the left and a watermark portrait of Franklin on the right.

Issuer Contacts

Credit Cards: VISA	1 (800) 367-8472	MasterCard	1 (800) 231-1750
Diner's Club	1 (800) 347-3102	AmEx	1 (800) 528-2121
Travelers AmEx	1 (800) 525-7641	Bank of America	1 (415) 622-9928
Checks: Citicorp	1 (813) 623-4618	MasterCard	1 (800) 223-7373
Visa	1 (800) 227-5353		

Bank Checks: Contact the check printer and the bank the check is drawn against.

Currency: Contact the local office of the Secret Service.

Real Stories from the Field

Credit Cards

General Fraud

A victim was at home in Chicago when \$1,200 from her Visa was taken out of a bank branch in Santa Barbara, CA. And since she never noticed her Visa card missing, she believes someone managed to get hold of her number and create a counterfeit card. She is currently in a dispute with her bank about who should pick up the tab.

U.S. losses from credit-card fraud are approximately 18% of issuers' cash flows from merchant fees, card fees and interest paid. Credit-card fraud is growing rapidly, alarming consumers and often putting big holes in their credit records. Experts estimate card fraud in the U.S. ran close to **\$1.3 billion in 1994, up from \$ 1 billion in 1993 and \$864 million in 1992.** Increasingly sophisticated thieves are coming up with a bewildering variety of ploys to rip off card holders and card issuers. As soon as Visa, MasterCard, and the issuing banks tackle one type of fraud, the bad guys come up with something new.

The worst abuses involve counterfeit cards. MasterCard's losses from counterfeiting reached at least \$113 million of its total \$395 million in worldwide fraud losses in 1993. Visa International's counterfeit losses were roughly \$160 million in 1993.

Counterfeiting

Counterfeiting costs consumers millions of dollars each year. Law-enforcement officials are increasingly frustrated by how easy it is for criminals to produce and use counterfeit cards. Some of the counterfeiters' schemes are shockingly simple. Counterfeiters were using gambits including bribes of employees at stores and mail-order houses to get card numbers. They then produced fake cards and enlisted accomplices to fly to other regions and get cash advances from banks. One group doing just this managed to steal millions.

Other counterfeiters are more sophisticated. For example, they focus mainly on gold cards because of their high credit limits. They target members of some groups with cards through associations, such as veterans, who tend to pay their bills regularly and have lots of unused charging power. Counterfeiters come up with account numbers and names, often by stealing receipts, and use easily obtainable encoders to make magnetic stripes that include this

information. They then affix the stripes to credit-card blanks or to genuine cards they have stolen.

Credit cards have so many different designs, and counterfeit cards are such close replicas of genuine plastic, that it's almost impossible for a store clerk to tell whether a particular card is legitimate. Even the holograms on the front of the cards, introduced in the 1980s to make cards harder to copy, are ineffective. Counterfeit holograms are coming out of the Orient by the bucketful.

Many rings of counterfeiters have flourished for years by maintaining tight secrecy. For example, groups of West Africans, many from Nigeria, have often been rounded up when they have tried to use counterfeit cards. Frequently, the would-be users tripped up on cultural differences between their countries of origin and the U.S., such as signing papers with just one name. But while they have nabbed some low-level members of these rings, law-enforcement has been hard pressed to finger leaders. Typically members refuse to help law-enforcement officials.

One thing that makes counterfeiting so easy is poor screening of cards when consumers make purchases. Many sales clerks, for instance, don't compare the data contained in the magnetic stripe on the back of a card (including name, account number, and expiration date) with information embossed on the front. On many counterfeit cards, the data does not match. Some stores have readers that display the magnetic-stripe information, but many do not.

Card issuers have started adding new, hard-to-copy codes to the magnetic stripes on new cards. But often, a merchant's card reader or a card processor's software will fail to read the codes correctly, and the issuer must fall back on verifying name, account number, and the like instead of checking for accurate codes.

Some changes are under way. Visa and MasterCard now require issuers to use the new codes. Both card associations are also trying to encourage merchants to update their code scanners so they can read the codes more accurately. They charge higher rates for old-fashioned processing and shopkeepers could be liable for fraud losses from transactions that occurred in their stores if those transactions involved cards with new codes that were not successfully screened. The new codes are helping. At Visa, which was the first to offer the new markers, counterfeiting losses **grew by only 15% worldwide as opposed to the previous year's 23%.**

But the new codes do nothing to protect consumers and issuers against skimming, a growing form of counterfeiting that occurs when someone actually gets hold of a card and copies, or skims off, every bit of information on a magnetic stripe including the new hard-to-copy codes.

And even if the card associations and the banks get a handle on counterfeiting, thieves will doubtless find other ways to operate. Issuers have managed to reduce the theft of cards sent to consumers through the mail. But professionals predict thieves will turn their attention to fraudulent card applications and away from counterfeiting. Others may attempt to steal cards by filing false change-of-address notices on valid accounts and asking for new cards.

And, as technology moves in the next few years from magnetic stripes to microchips, the ability to compromise a specific card will be greatly reduced. However, history has shown us that criminals are resourceful, constantly coming up with new scams to catch the vulnerable.

Scams

One that surfaced during the recent holiday season involved callers claiming to be a major catalog company with a special offer: Order from us now and claim an on-the-spot discount. People who stopped to think realized that catalog companies don't call customers, especially at the busiest time of the year. Others, blinded by the prospect of a discount, gave their credit card numbers and saw fraudulent charges on the next statement.

Another recent scam involved an auto dealership asking customers, even those who were just looking, to fill out a preliminary application. Armed with names, addresses and Social Security numbers, employees applied for credit in the customers' names and ran up sizable bills before they were caught.

In another twist, a change of address scheme hit the Midwest very heavily. In this scam, which hit fast and hard, and caught a lot of people off guard. Thieves picked credit card statements out of the mail, then called banks to report a change of address. With statements sent to the new address, considerable damage was done before the cardholder found out.

Other scams are perpetrated by so-called "dumpster divers" who hunt through trash for discarded credit card receipts and credit card offers. A store clerk may give you a hard time, but Visa and MasterCard regulations, and the laws of several states, prohibit merchants from requiring personal information as a condition to accepting your card.

Nigerian credit bandits are plaguing U.S. card users and eluding the legal system. Last month's credit card bill didn't arrive? The bill may have been diverted to a Nigerian crook in any one of a dozen U.S. cities, and he could already be milking the account for cash. Law-enforcement officials say the credit card industry is under siege from a loose network of Nigerian criminals entrenched in cities including New York, Houston, Dallas, Atlanta, New Orleans, and Los Angeles. The West Africans' sophistication and their ever-changing techniques developed a change-of-address scam that is causing big headaches for the Secret Service, the Immigration and Naturalization Service, and credit card issuers. Nigerian officials angrily reject such talk as offensive and untrue, insisting that the vast majority of their citizens here are law-abiding residents. In fact, they assert, many so-called Nigerian criminals are actually other West Africans masquerading as Nigerians for reasons that aren't clear. But U.S. officials say the Nigerian crime wave is real--absolutely epidemic according to a Secret Service Agent. Law-enforcement officials have arrested more than 1,000 Nigerians since record keeping started in 1989, accounting for fully 10 percent of the fraud arrests made during that period by the entire Secret Service, which heads a national task force formed to deal with West African crime. The low-profile task force, which has members in 13 cities, has recovered nearly \$50 million in money stolen by Nigerians. But agents believe they've tracked down only half the loot from the crimes they've solved. Much of the rest may have been spirited out of the country. According to task-force members, the Nigerian credit crooks are neither hierarchical nor territorial but work in loose bands of 3 to 15. They frustrate local police by shuttling between various jurisdictions, keeping meticulous records, and sharing the details of their high-tech scams with members of other cells. According to several law officials, many train in special "boarding schools" in New York, Houston, and Atlanta after arriving in the U.S. to make a living from credit rip-offs. The latest wrinkle in Nigerian fraud is the change-of-address scheme. With just a person's name, the name of the financial institution, and an account number or Social Security number, it's easy to change the address of any credit card account--and from there, to change the secret code number that allows card users access to a cash machine. By tapping the new information into a gadget that encodes the magnetic stripes of old or fake cards, the outlaws create their own duplicate cards. A practiced card shark with a fistful of fake cards can walk away from a cash machine with more than \$10,000. The crime is ingenious and nearly risk-free. A national task force is making some progress. For example, agents in Washington, D.C., alone busted 40 people, mostly Nigerian, who were allegedly working as credit bandits. Authorities think the crooks bagged as much as \$10 million from thousands of accounts, in part through the change-of-address ruse. But by using cards hijacked in other parts of the country--and by limiting the amount of money they steal in any jurisdiction--most Nigerian criminals escape the attention of an overburdened system or just leave the country.

Future Technology

What's noise to one person is music to another. In fact, the "noise" in the magnetic strips on credit cards could soon be sounding sweet to banks by helping them cut down on credit-card forgery. Researchers discovered that even tiny patches of magnetic media contain a pattern of minute magnetic particles as unique as a fingerprint. Today's credit-card readers are designed to screen out the noise caused by these particles and concentrate on the recorded data. But with an inexpensive semiconductor chip, readers can pick up and analyze the noise signal, extracting a card's magnetic fingerprint to verify whether it is genuine. The technique can't prevent stolen cards from being used, but credit-card forgery now costs banks hundreds of millions a year.

Why not encode a picture of the cardholder on the card's magnetic strip? Unlike photos, the digitized image would be hard to alter. When the card was swiped through a reader, the image would pop up on the clerk's screen. In late March, Kodak announced that its scientists had compressed a human facial image two-hundred fold, down to an incredibly tiny 50 bytes, just small enough to fit into the unused storage space on a credit card's magnetic strip. Two blue-chip partners, Citicorp and IBM, plan to test Kodak's system with customers in the near future. The system provides two levels of security. A salesclerk can catch obvious fraud by comparing the picture on the checkout terminal's screen against the person who presents it. Beyond that, a series of bits derived from the portrait, called a verification code, is sent to the bank along with the usual data, such as the sale amount. If the code doesn't match what the bank's computer expects, the transaction is rejected. The code changes with each transaction, a big advance on current static codes that can be easily forged. Result: Even if a clever thief managed to fool a clerk by encoding his own portrait on the strip, he would still be caught by the bank computer. It's like a door with interconnecting locks, It won't open without both keys. The digital photograph is dealing with just one type of image: a face. It would have two eyes, a nose, a mouth, hair, and so forth, thus limiting the information needed. The method starts with a low-resolution image of about 10,000 bytes. Then it squeezes it, using a police-sketch type of algorithm. The algorithm breaks down the image into small portions and then finds ones that match, so the overall face can be represented more compactly. Of course, it's more complex than that, and there is software that blends features to deliver a more lifelike portrait. Some new point-of-sale terminals can be converted to use it for as little as \$500. Photos could be taken at bank branches or gathered from motor vehicle departments. It's less intrusive than scanning fingerprints or retinas and more fraud-proof than electronic signature pads.

But a photo-security system works only for face-to-face transactions, currently just 60% of all sales on the Visa International network and shrinking. What's more, both Visa and MasterCard International Inc. plan to phase out magnetic-strip cards in the next decade, switching to smart cards with computer chips that can store far more information. Smart cards are credit-card sized devices that use tiny embedded computer chips to store data and digitized currency. They are expected to become widely used in the U.S. and elsewhere as electronic "purses" for cash transactions, in access controls for buildings and equipment, and for identity authentication for documents transmitted over computer networks. It's not clear if many banks or retailers will spend money converting to Kodak technology that could soon be obsolete. Visa also reports that credit-card growth fraud on its global network has shrunk about 20% in each of the last two years, thanks to new security measures, such as software that detects aberrant spending patterns for an individual card. And banks and retailers don't know how customers will react to having their picture so widely used.

The US West Telecard looks like a credit card, but embedded in it is a microchip that can be loaded with digital cash for use in pay phones throughout Seattle. By next summer, 16,000 specially equipped pay phones in five cities will accept the cards. Now the company is talking with retailers. It's a win-win situation: Consumers get added convenience; U S West gets the promise of higher revenues. In fact, this is an idea that's two decades old--the smart card, so called because of the microchip that puts information in the card. Patented in the 1970s, by the 1980s they were heralded as the next breakthrough in electronic payment technology--not just as high-tech cash cards but to enhance credit cards to prevent fraud and store information, such as medical records. Despite studies showing that consumers would leap at the chance to carry cash on plastic, and despite successful launches such as U S West's, they have yet to spread nationwide. Thanks to a handful of innovators, the smart-card movement is beginning to pick up steam. There are obstacles, but they are likely to be overcome. Part of the reason for the cards' bright future is global travel. Smart cards have taken off all over Europe and Asia: Most of the nearly 33 million of them in circulation by yearend 1994 were issued there. The French have shopped and telephoned with smart cards for nearly a decade, and they're popular even in Russia. There are more chip cards issued than magnetic-stripe cards in Moscow. MasterCard and Visa are both launching smart cards internationally. Another factor encouraging the spread of these cards: They're a handy way of processing penny-ante transactions. Last year, some \$1.8 trillion was spent worldwide on purchases of under \$10, some \$560 billion of that in the U.S. Such transactions represent a huge potential market for cash cards. Both merchants and consumers stand to benefit, but no one has been willing to ante

up for the expensive equipment needed to process the cards until they become more widely used. Smart cards, while profitable, would not generate as much income as credit cards.

A consortium of major Japanese banks and credit-card companies will launch a large-scale trial of an electronic cash-card system with Visa International Inc. Japanese credit-card companies DC Card, UC Card, Sumitomo Credit Service, Credit Saison and Million Card Service and Bank of Tokyo-Mitsubishi Ltd., Dai-Ichi Kangyo Bank, Fuji Bank Ltd., Sumitomo Bank Ltd. and Tokai Bank Ltd., will use Visa's version of a so-called smart-card system. The Visa cash cards will be used in the Shibuya district of Tokyo. Shibuya was chosen because of the number of shops, restaurants and theaters in the area, and because it is an area young people frequent. While Visa plans to introduce an electronic cash card in the Kobe area of Western Japan soon. the Shibuya venture will be much larger in scale, and the first to have joint cooperation from several Japanese city banks.

Rival credit-card association MasterCard International recently acquired a majority stake in a London-based smart-card technology concern Mondex International. and American Express Corp. is also working to set smart-card standards. Smart-card technology is commonly used in Europe, both at automatic tellers and at cash registers. An estimated two billion smart cards are expected to be in circulation worldwide by 2000, according to experts. More than 300 million cards with computer chips were issued in 1993 alone, for use in phones, health care, banking and pay-TV services. Smart cards have been touted as a tamper-proof solution to computer security but some researchers say they are vulnerable to attacks by sophisticated hackers. Despite the vulnerabilities, smart cards are far more secure than common magnetic-stripe cards, such as credit cards, which are easy to counterfeit. Unlike magnetic-stripe cards, which simply store data, smart cards contain a chip which generates a digital key used to encrypt data.

Checks

Technology of Checks

Check Standards Resource: If you're interested in more of the technical details and specifications of check printing, source the following documents;

- ANSI - American National Standards Institute X9 Committee
- ABA - American Banking Association (Center for Banking Information)
- CBA - Canadian Bankers Association.

U.S. Check Standards are published by The Accredited Standards Committee X9 on Financial Services. To order call the ABA at 202-663-5087.

Documents Available Include:

- Bank Check Background and Numerical Convenience Amount Field (X9.7, Catalog #092100)
- Specifications for Placement and Location of MICR Printing (X9.13, Catalog #090400)
- Paper Specifications for Checks (X9.18, Catalog #091100)
- Print Specifications for Magnetic Ink Character Recognition (X9.27, Catalog #092200)
- Understanding and Designing Checks (X9/TG-2, Catalog #092600) Canadian Standards and Specifications for MICR Encoded Documents are published by the CPA (Canadian Payments Association). To order call the CPA at 613-238-4173.

MICR: Checks are printed on a variety of paper stock and backgrounds but all must include MICR printing (Magnetic Ink Character Recognition).

MICR Fonts: MICR fonts meet ANSI (American National Standards Institute) and ABA (American Banking Association) standards. All fonts have been designed for Hewlett Packard LaserJets and compatibles.

MICR Overview: MICR characters are the unusual small block shaped characters at the bottom of each check. These magnetic characters allow your bank's Reader/Sorters to identify the account, institution number, and check number very quickly. Traditionally MICR documents have been printed with a special ink with a high iron oxide content that was only available to specialty printers. In the 70's MICR toner was developed for large mainframe printers such as the Xerox 9097. These printers cost hundreds of thousands of dollars. Finally in the late 80's MICR toner was developed for desktop laser printers. Laser printed MICR checks can be printed with almost any Hewlett-Packard LaserJet printer, a MICR toner cartridge, a MICR font, the proper software, and blank check stock.

A standard toner cartridge does not have enough iron oxide in the toner to produce a high enough signal strength for the checks to pass through the banking system. ANSI check specifications require that checks have a minimum signal strength of 50%. Regular toner cartridges will not produce the MICR characters with a high enough signal strength and will have to be manually encoded (attach an additional magnetic strip at the bottom of the check).

These checks can be analyzed with a MicrMate check analyzer to verify that the checks signal strength exceeds ANSI and ABA (American Banking Association) standards, so checks will properly clear the system.

Do laser printed checks cost more than pre-printed check stock? Absolutely Not! MICR check stock typically costs 5 cents each, plus the MICR toner costs approximately 2 cents per page. A total cost of 8 cents a page, on the high side. This example assumes you are printing only one check per page on a Hewlett Packard LaserJet III. Printing costs may be lowered if you print multiple checks per page, depending on the check stub needs. Pre-printed check stock typically costs \$100 per thousand.

MICR Character Placement Gauge: The most common reason for rejected MICR documents is character placement. Either the characters are not where they are supposed to be or other information such as the signature or address have found their way into to bottom 5/8" of the check. Character placement is crucial to a quality MICR document. A typical gauge consists of a thick sheet of lexan with a mylar overlay that is silk screened with the proper placement layout. Just insert the document and you will instantly know whether your documents meet ANSI MICR character placement standards.

When producing MICR checks in quantity, quality control becomes an issue. Purchase a MICR document verifier. A MICR verifier scans a MICR document and analyzes it to make sure it meets ANSI standards. Most verifiers check signal strength, character wave form (shape), and character placement. These verifiers range anywhere from \$300 to \$5000 depending on options. Most end users don't really need a verifier if they are purchasing their toner, fonts, and software from a reliable source. However, if you need a verifier, there are several companies that produce good products that should fit your needs.

Check Counterfeiting

With the advent of ever more sophisticated copying machines, check counterfeiting has become the crime of the 1990s. The U.S. Justice Department estimates that \$10 billion worth of bad checks are passed every year.

Financial fraud is growing, forcing banks and individuals to find new ways to protect themselves. The passing of fraudulent checks alone surged 136% between 1991 and 1993. The estimated cost to the nation's banks was a whopping \$815 million. Sophisticated desktop-

publishing software, scanners, laser printers and color copiers have contributed to the problem, according to the American Bankers Association's Check Fraud Task Force.

Checks used to be fairly safe, but, like cash, counterfeiters can now duplicate checks with amazing accuracy.

Because there is no single standard and they can be printed in many different ways, checks are much easier to copy than credit cards. Many large companies, in fact, print their own checks. Payroll check fraud is rampant. A Los Angeles gang recently roamed the nation cashing counterfeit payroll checks to the tune of nearly \$25 million. Executives are just as vulnerable as corporations to such scams. A Boston gang recently got the names and birth dates of executives from "Who's Who" listings. They then applied for credit cards and loans in the executives' names. Newly opened accounts can drain banks as criminals deposit a phony check and draw on it before the fraud is discovered. To stop this activity, banks are increasingly requiring at least two pieces of personal identification on new accounts. Some are also delaying checkbook orders and the issuance of ATM cards until references have been verified. Another step banks are taking to stem check rip-offs is the use of built-in check security features. Individuals should benefit from new check guidelines issued by the Financial Stationers Association, a Washington-based trade group for check printers. Among FSA's recommendations are micro-printed data and a lightly printed "security screen," which can't be picked up by a color copier or laser printer. Checks bearing these marks may have a small padlock symbol on the front. Some institutions are starting to require use of the bank's vendor when ordering checks. This may well annoy some customers accustomed to ordering lower-cost checks from outside vendors. Where banks have this rule if non-bank checks are used and then involved in a counterfeit attempt, the customer may be liable. You have to be alert, too. Protect your account information. Try to limit the amount of personal information that appears in any one place. Don't print your phone number or driver's license number on your checks. And refuse to write a credit card number on a check even if a sales clerk asks for it. All this information in one place leaves you open to fraud. Protect checks and credit cards as if they were cash. Report lost or stolen checks. Review bank statements as soon as they arrive. Don't be lax about reviewing statements. They will tap into a number of accounts and take a portion of each, not bleed one account dry. Store canceled checks in a safe place. Tear voided checks in small pieces before discarding. Be just as careful with deposit slips. Be careful when you're given checks. The seller of a used car who is smart enough not to take a personal check can be victimized by a counterfeit certified check.

A certified check is the easiest thing to fool around with, it's not a good safeguard anymore. If you take a check from a stranger in this kind of situation, walk the person into the bank and get the cash before signing over the car title. If this isn't possible, hold onto the title until you've cashed the check.

Put ATM receipts with your account number in your pocket instead of leaving them near the machine. Be careful when you use a cash machine or enter a card number into a public telephone. "Surfers" can get your account number and make illicit use of the data. When a thief steals your credit card, you're liable for no more than \$50. Similarly, consumers are protected from check fraud. If your checking account number has been compromised, if someone has assumed your identity or stolen your checks, you're protected and the bank takes the hit. However, it's much like being rear-ended in a car accident. It may not be your fault, but you have to work hard to rectify the problem.

The Future

There's no doubt banks would save money if they could scan checks and send them electronically to each other. Transporting physical checks, either by air or ground vehicles, is the largest check-settlement cost for many banks. But electronic check imaging isn't just a cost-cutter, it promises to reduce check fraud, too.

Recently a system was demonstrated that lets banks trade check images (of checks) electronically, no matter what kind of computers they use. The check imaging research is helping the banking industry in areas beyond check processing.

Imaging It makes key information available faster. Consider if a check was presented in California that was drawn on Citibank. It could take two days before Citibank would see that item and mark it as suspect. If you could capture the information electronically when (the check) was deposited at the branch, it could be shipped in a few hours.

This will change check process because today, in most cases, check imaging is used internally inside banks. Most banks still rely on the physical checks to come in before they do anything with them. The breakthrough is in the return process. We have technology now to deliver an image at a high enough quality to an operator and use that image as opposed to the physical check.

A barrier to wide spread use of imaging technology is not standardized. Take the example of the (companies that took part in the) presentation. One bank uses IBM equipment today to capture and store image information. Another bank uses Unisys equipment, and a set of different compression algorithms and file formats.

Compression technology can also help A good example is a credit card application. The application can be scanned in and compressed. In addition, the credit card information can be sent to the credit history people and the people making the database of customer profiles. Just like a check can be processed by several people simultaneously, so too can the application be sent to several places in a bank and processed at the same time.

Imaging technology can also help with intelligent or optical character recognition. It's being planned to be used to decipher handwritten information on checks. But it's also ideal for reading documents, such as credit card applications.

Currently there's clearly a momentum moving away from physical checks to digital technology. There is a lot of hardware and software out there to deliver check imaging. Banks are in various stages with this technology. Most banks need to make banking information available 24 hours a day, seven days a week and have begun doing so. Imaging technology will be "another piece in the puzzle" in helping banks achieve rapid information availability 24 hours per day.

Currency

Counterfeiting Is On The Rise, As A Result Of Today's PCs And Printers

The Family Farm Preservation, based in Tigerton, Wisconsin, seems like just another radical fringe group. Members of the FFP believe paper money is worthless because they believe the Federal Reserve, which issues currency, is illegal. However, the FFP is taking its beliefs one step further. The FFP has helped launch a campaign to circulate counterfeit money orders to expose what they believe to be the fraud of the current monetary system.

The money orders, duplicated on photocopying machines, looked real enough that an unidentified California lender lost more than \$30,000 when it released title to two cars before determining the orders were fraudulent, according to state regulators.

Many financial institutions these days are finding that counterfeiting is far more than a nuisance. Whether it's fraudulent money orders, corporate checks, travelers checks, or fake securities posted as collateral for loans, document fraud is on the rise. According to the Secret Service's Financial Crimes Div., losses to banks from fraud cases under investigation doubled in 1993, to \$1.4 billion. Agents say much of that increase is the result of counterfeit negotiable instruments.

The boom in document fraud stems from the ready availability of computers, laser printers, and color copiers. With these machines, even relative novices can produce replicas of currency and other similar instruments that are often just as hard to detect as documents created by skilled counterfeiters. The instruments being produced now are very deceptive.

The cost of counterfeiting to the financial services industry is hard to measure. However, estimates of losses from check fraud alone, by far the most costly and widespread form of document fraud, run as high as \$10 billion.

Increasingly, check-fraud rings are targeting corporate business accounts. Once a group has obtained a copy of a corporate check, often by fishing through dumpsters for discarded checks or by stealing them from mail drops, the check is scanned into a computer, where both the amount and the payee can be altered. Using check paper and magnetic ink that is readily available in office-supply and computer stores, rings produce a nearly undetectable forgery. And with government rules requiring most checks to clear in a maximum of five days, money is often withdrawn before a bank or corporation realizes phony checks have been cashed.

The high-tech robbers often operate nationwide. Recently the Secret Service arrested 30 people tied to a Vietnamese gang in Southern California. All have been indicted. One government investigator says the group counterfeited corporate checks on laser printers and recruited people in at least five states to cash them. It cost a large California bank \$2 million in losses.

Other negotiable instruments, such as stock and bond certificates, are also being forged with growing sophistication. Law-enforcement officials say they are exploring a growing number of cases where loans were issued based on phony securities used to bolster an individual's net worth or as collateral.

Some doctored instruments may not even be counterfeits of legitimate securities. Over the past several months several people were arrested after they tried to use counterfeit Japanese bond securities, instruments the Japanese government has said never existed, to obtain a \$900 million letter of credit from a U.S. bank.

Banks are now stepping up development of high-tech counterattacks against counterfeiters. In April, American Express Co. introduced a redesign of its traveler's checks, which will include a hologram of a globe that can't be picked up by a photocopy. And nearly two dozen of the nation's largest institutions have signed on to a new system called CheckLink, which tries to detect fake checks before they clear.

The Money Supply

In case you haven't noticed, something strange is happening to the most tangible component of the money supply--the good old American greenback. After posting healthy gains in the early 1990s and indeed, during most of the postwar period, growth of currency in circulation slowed sharply last year. It is now expanding at its slowest year-to-year pace in more than 30 years.

It's uncertain whether the slowdown in demand for paper currency is telling us something about foreign economies, the U.S. economy, or perhaps both."

More and more greenbacks are exported, legally or covertly. Dollars are used for transactions not only in Panama and Liberia, which have adopted the dollar as their official currency, but also in Latin America, Eastern Europe, and the Middle and Far East.

The Federal Reserve estimates that as much as 70% of U.S. cash in private hands (currently about \$375 billion) may be held outside the U.S. More important, they say, some 80% of all currency growth since 1980 seems to be tied to rising foreign demand.

The big impetus behind such demand, of course, has been political and economic turmoil overseas, such as the breakup of the Soviet empire and the economic crises enveloping Latin America a few years ago. In fact, many experts attributed the slump in currency growth last year to unfounded Russian fears that American plans to issue a new counterfeit-resistant \$100 bill would somehow affect the value of old bank notes. Thus, when the new U.S. C-note was finally issued this March, the betting was that demand for bank notes would start to accelerate again.

The fact that demand for U.S. currency has continued to languish--at least thus far--suggests an intriguing thesis ... that is ... growth in U.S. currency seems to have become an index of international political and economic instability.

If that's true the current slowdown in demand for U.S. bank notes may be signaling the recent success of economic and political reforms in Eastern Europe and Latin America.

University Students Learn How To Make Money: Just Copy It

Three Columbia University students and a non-student were charged with using a school color copier to crank out \$85,000 worth of counterfeit \$20 bills in late 1996.

The bills were being passed successfully at local businesses. They were "not really high-quality counterfeit notes, but if the public will accept them, it's a problem, he said. The suspects were planning to print an extra \$200,000 of bogus bills and sell them in New York, Chicago and Washington.

Two of the men were roommates, and a federal complaint said counterfeit cash was found in plain view in their apartment, including on the table in the living room, and a stack of bills in an open cabinet in the kitchen.

The Secret Service first spotted the bogus bills in May, after some were passed at a bar. Technicians recognized the counterfeits as the products of a particular type of copier, which was traced to a printing office in the basement of the University's Journalism School.

The Super Bills

A ring of Iranian and Syrian counterfeiters is printing near-perfect \$100 bills faster than the U.S. government itself, that brought an end to the old currency.

The founding father's face had graced U.S. currency virtually unchanged for the past 80 years, until recently, and the \$100 bill has reigned as the highest U.S. denomination since the \$500 bill was withdrawn from circulation in 1969.

But Ben has been in danger ever since "the high-tech \$100 bills," as a Federal Reserve Bank spokesman calls them, started appearing. Their quality is so good that for several months, the Fed quietly honored any fake "superbills" submitted by banks for exchange or collection. That unprecedented suspension of policy was never publicly disclosed. It ended when the banks

finally had enough experience to start identifying the "superbills" themselves --the usual practice for identifying counterfeit notes in circulation.

Two congressmen even pushed for little-noticed legislation that could lead to the complete withdrawal of the Franklin bill, a move that's favored by the Drug Enforcement Administration. The rationale for such extreme action: Working out of Lebanon's Bekaa Valley, the counterfeiters already have produced as much as \$1 billion in "superbills", described as the best U.S. currency ever made outside the Bureau of Engraving and Printing. They're perfect down to the magnetic properties of the ink. To compare only \$300 million worth of real \$100 bills was printed last year.

The "superbills" have thrown top U.S. officials into a panic. For good reason: There's an outside chance the dollar could be de-stabilized by this flood of counterfeit money--although that would require truly massive quantities of fake notes to be injected into the world economy, a rather far-fetched scenario.

More likely, though hardly less worrisome, is that the funny money is being produced to buy weaponry. CIA officials and terrorist experts believe the governments of Iran and Syria are masterminding the operation so they can buy weapons from North Korea, China, or rogue elements within the former Soviet Union. Syrian officials deny any involvement; representatives of Iran, North Korea, and China have no comment.

Experts say the only sure way to slow the Bekaa ring is to alter radically, or just do away with, the old-fashioned C-note. Minor changes didn't work: The bill was retooled twice to deter counterfeiters. The first retooling adding a polyester strip that reads "USA 100" when held up to a light. The second retooling resulted in the modern currency we see now. The "superbills" don't have such a strip but have "USA 100" Imprinted so cleverly it's hard to tell the difference.

Legislators and government officials are focusing on damage control. A "superbill" committee is examining the issue, and a measure cosponsored by congressmen ordered the Treasury Department to devise ongoing solutions, however extreme. Among those arguing for the death of the \$100 bill has been the DEA, which has always hated the large denominations used by drug traffickers. In this case, the fake notes apparently are continuing to move into circulation via well-tested drug routes out of the Bekaa Valley.

The Bekaa counterfeiting ring ultimately helped reshape U.S. currency. Whatever their solution for the "superbill" problem, government officials will likely have to continue to reevaluate the security of all U.S. paper currency.

Glossary of Terms

The following is a glossary of terms as they relate to counterfeiting and document review.

Artificial Watermark	This is usually a very light screen printed on the back of some checks. It can also be a very light, or just off-white color ink.
BIN Number	The BIN number is the credit card Bank Identification Number for the issuing bank. It is four digits long and is the first four digits on a VISA. The BIN number will also be printed in ink either above or below the embossed number and it will be included in the microprinting around the VISA logo.
Blanks	Credit cards that have not yet been embossed. All major credit cards are printed on white plastic core stock.
Check Digits	These are digits that are used to "check" a document. They usually relate to a coded message and must come back to the issuer of the document for verification.
Coding	The process of placing a code on a magnetic strip of a credit card.
Copiers	Primarily color copiers are used in counterfeiting. A copied document will have a shiny texture and the toner will rest on top of the paper, not in the paper. Also, there will usually be no actual paper visible, at least with currency, since the copier will fill in with toner any area that is not white. Also they are unable to reproduce fine line detail, holograms, kennegrams and microprinting.
Core Stock	This is the core of the document. On most major credit cards it is white plastic. It will vary on other documents such as bank checks, travelers checks, etc.
Design	This is the overall design of the document to make it both readily identifiable as genuine, and difficult to reproduce or counterfeit.
Embossing	The process of raising the surface of a document to either give texture or so it can be read mechanically.
Encoder	A piece of equipment used to code the magnetic strips on credit cards and similar cards.
Etching	The process of removing a portion of the service of a plate that will be used in printing.

Fibers	Threads or fibers inserted into paper in the process of making paper that, when the paper is finished, can be used to both identify the document and check its authenticity. Examples are the denomination fiber and the red and blue fibers in currency.
Fine Line Printing	Using lines for both texture and shading, fine line detail is difficult to reproduce by a copier, but can be reproduced, to a degree, with photolithography and offset presses.
Foil	A very shiny surface applied with thin sheets of colored plastic or metal. The foil is usually on the raised - embossed - characters on credit cards and some travelers checks; bank checks and foreign currency are now using foils.
Hologram	A laser produced image that shifts when viewed from different angles. An example is the hologram dove on the VISA card and the hologram globe on the MasterCard card.
Inks Magnetic	Magnetic ink is used on checks for the MICR printing and on the face of U.S. Currency.
Inks Ultraviolet	An ultraviolet ink is invisible to the naked eye but can be seen under ultraviolet light.
Intaglio	It is a process of reverse image printing on special intaglio printing presses to produce ridges of ink on the surface of the document. It is the intaglio process that gives travelers checks, currency, and some stock and bond certificates the feel of money.
Kennegram	It is similar to a hologram, but the image doesn't move; it shifts from one image to another image. An example would be a bust facing right then facing left when viewed from different angles.
Laminate	The process of combining two or more layers to produce a final finished product. Examples are the new hundred dollar bill, credit cards with chips inside, or plywood.
Laser Scanners	There are two primary types of laser scanners, the commercial desk top and the industrial drum scanner. The commercial desk top scanners are not able to reproduce the fine line detail. The industrial drum scanners, made primarily for the semiconductor industry can.
Lithography	The process of producing an image on a specially prepared surface, usually zinc or steel for counterfeiting. The process produces unusually high quality images.

Magnetic Strip	A piece of metallic oxide imbedded in a plastic tape and adhered to the back of a credit card or similar type item.
MICR Printing	Magnetic Ink Character Recognition are the unusual block characters seen on the bottom of bank and travelers checks.
Microprinting	Printing that can't be readily seen by the unaided eye or any copier or commercial scanner.
Offset	A type of printing where the image is positive and is offset to a third roller before printing on the document.
Paper Making	A process where by fibers are combined in a liquid state with adhesives and binders and then poured or laid out on a screen to first drain and then dry. The paper can then be further processed.
Photograph	An image of a person either in film or digital image.
Polaroid One to One	A camera that can reproduce an image exactly the same size as the original. This camera was designed for commercial ID's but has been used to counterfeit ID's and credit cards.
Raising	The process of washing all of the ink from lower denomination bill and re printing the bills as higher denomination bills. This involves raising singles to 100's
Reverse Italics	A type of printing wherein the characters lean to the left. It is used to print the account number on the signature strip.
Security Screen	A lightly printed image that can be read with the unaided eye but cannot be seen by a copier or scanner.
Signature Strip	A strip on the back of credit cards that will hold an ink signature. The strip usually has some form of overprinting. When erased the overprinting will disappear and show a warning or will say "Void" underneath the signature strip. Fake signature strips are usually flat white paint and may have been silk screened over with the light overprinted characters. This can be felt since silk screening and painting both produce relatively thick finishes.
Silk Screen	A process of forcing ink through a fine mesh silk screen that is not blocked by a resist.
Surfing	The process of swiping a card for just its information and not part of a commercial process.
Watermarks	A process in making paper that shifts the density of paper fibers to produce an image when held up to the light. It is a very common feature in bills world wide.