

LIST OF DOCUMENTS PRODUCED TO EFF FOIA REQUEST

1. Office of Financial Records Travel records
2. Central Bank Counterfeit Deterrence Group two (2) page press release dated January 9, 2004.
3. Three (3) page email dated April 22, 2007, from Larry Felix to Dawn Haley regarding Central Bank Counterfeit Deterrence Group.
4. Two (2) page email document with attached press release dated March 31, 2008, from Lenore Clark to Edmund Choy, Trucchi Huynhtran, Ladislav Falat, John Hallocj, Daniel V. Humphrey, Dave Cornell, David Curtis and Ted Strahan regarding tracking counterfeits through laser printers.
5. Letter with attached documents to Director of the Bureau of Engraving and Printing dated November 30, 1995, regarding use of electronic scanning, bar coded currency and databank monitoring to detect and deter counterfeiting and money laundering.
6. Three (3) page facsimile cover sheet with 18 page attachment dated June 3, 1998, regarding Agenda for the June 12, 1998 Plenary SSG-2 Meeting in Stockholm.
7. Two (2) page distribution list of the Tracing System.
8. One (1) page letter with attachment (Executive Summary of SSG-2 Activities) from Banque of France dated July 21, 1995.
9. Four (4) page facsimile regarding Executive Summary of SSG-2 Activities dated July 21, 1995.
10. One page Cover Memorandum with three (3) page attachment regarding the Advanced Counterfeit Deterrence Steering Committee of July 11, 1995.

11. One (1) page facsimile cover sheet with attachment (Agenda) with facsimile confirmation dated June 2, 1998 regarding Agenda/Summary for Plenary Meeting.
12. Three (3) page facsimile cover sheet with five page (5) attachment dated June 17, 1998, regarding the Minutes of the June 12, 1998 Plenary SSG-2 Meeting in Stockholm.
13. Three (3) page email from Eugenie E. Foster of the Federal Reserve Bank titled "Cat's out of the bag" dated January 8, 2004.
14. One page email from Eugenie E. Foster of the Federal Reserve Bank dated January 6, 2004.
15. One page email from Eugenie E. Foster of the Federal Reserve Bank regarding high definition images dated January 21, 2004.
16. Two page email dated January 14, 2004 regarding media interest in printer issue.
17. Two page Adobe Press release dated January 10, 2004, regarding anti-counterfeit technology in product.
18. One page memorandum dated January 9, 2004 regarding Media Inquiry regarding Counterfeit Deterrence System.
19. One page email dated March 9, 2004, regarding Central Bank Counterfeit Deterrence Group.
20. Two (2) page email dated January 12, 2004, regarding article titled "Adobe Helped Government Fight Counterfeiting".
21. Two (2) page email dated September 23, 2004, regarding response to media inquires regarding anti-counterfeiting technology in copiers.

22. Five (5) page email dated February 16, 2004, regarding recent stories regarding Anti-Counterfeiting technology.
23. Draft press release dated November 3, 2008, regarding Counterfeit Deterrence System (CDS).
24. Three (3) page mail dated January 16, 2004, regarding CDS technology.
25. One (1) page email dated January 13, 2004, regarding CDS.

CBCDG

CENTRAL BANK COUNTERFEIT DETERRENCE GROUP

Fax: +1-613-782-8184

Date: 9 January 2004

Important message

On 9 January 2004 there has been media inquiries in the United States about the CBCDG and the CDS (Counterfeit Deterrence System). The former CBCDG Project Director was also interviewed. Articles will most likely start to appear in newspapers soon. Questions may likely be directed at your central bank by various media.

Please ensure that the spokesperson for your institution responsible for communications about CDS are familiar with the attached communication program. Spokespersons should use the information provided in the Questions and Answers and the Key CDS Messages to respond to inquiries.

Please fax potentially urgent information published about the CDS to the Chairman as quickly as possible.

To:	Marc Salade	National Bank of Belgium	+32-2-221-3109
	Richard Wall	Bank of Canada	+613-782-8184
	Antti Heinonen	European Central Bank	+49-69-1344-7403
	Jean-Claude Gilles	European Central Bank	+49-69-1344-7403
	Yasuhisa Hashimoto	Bank of Japan	+81-3-5203-7307
	Tomoko Kurose	Bank of Japan	+81-3-5203-7307
	Roland Tornare	Swiss National Bank	+41-31-327-0221
	Eugenie Foster	Board of Governors of the Federal Reserve System	+202-452-6474
	Michael Lambert	Board of Governors of the Federal Reserve System	+202-452-6474
	Geoffrey Board	Reserve Bank of Australia	+612-9551-8017
	Wolfgang Färber	Austrian National Bank	+43 1 316 90 1499
	Vladimira Stoyanova	Bulgarian National Bank	+359 2 971 4667
	Leopold Surga	Czech National Bank	+42 02 2441 2834
	Leif Yde	National Bank of Denmark	+45 33 637 121
	Paavo Perttu	Bank of Finland	+35 89 183 3466
	Maurice Perron	Bank of France	+33 1 4292 3009
	Wolfgang Söffner	Deutsche Bundesbank	+49 69 9566 3289
	Ioannis Leventis	Bank of Greece	+30 210 672 2577
	Zsuzsanna Földing Magyar	National Bank of Hungary	+361 428 2519
	Louis O'Byrne	Central Bank & Financial Services Authority of Ireland	+35 31 295 6536
	Donato Pasquariello	Bank of Italy	+39 06 4792 7197
	René Link	Central Bank of Luxembourg	+352 47 74 4960

Henny van der Wielen	Netherlands Bank	+31 20 524 2526
Jan Erik Johansen	Central Bank of Norway	+47 22 31 66 58
Alicja Dukaczewska	National Bank of Poland	+49 69 1344 8672
Fernando Costa E Almeida	Bank of Portugal	+351 263 8513 04
Roberto Andrade	Bank of Spain	+34 91 338 6887
Michael Reizinger	Sveriges Riksbank	+46 8 21 05 31
Aykut Ekzen	Central Bank of the Republic of Turkey	+90 312 311 2953
Andrew Bailey	Bank of England	+44 207 601 3801
Lorraine Laviolette	Project Office	+613-782-8184
Bob Stone	US Bureau of Engraving and Printing	+202 874-3483
Kerry Davison	Bank of Canada	+613-782-8184

From: Pierre Cloutier
pcloutier@bank-banque-canada.ca

Number of pages, including this cover page : 21
If you do not receive all the pages, please call: +1-613-782-8904

Attached you will find the CDS Communication plan.

Haley Dawn

From: the Felix [felixlw@comcast.net]
 Sent: Sunday, April 22, 2007 11:47 AM
 To: Haley Dawn
 Subject: Emailing: CBCDG - Central Bank Counterfeit Deterrence Group

- ÄEesky
- Dansk
- Deutsch
- Eesti keel
- English
- EspaÄ±ol
- FranÄ§ais
- Italiano
- LatvieÄju
- LietuviÄ³ k.
- Magyar

- Malti
- Nederlands
- Norsk
- Polski
- PortuguÄs
- RomÄgnÄf
- SlovenÄjÄina
- Slovensky
- Suomi
- Svenska
- TÄ¼rkÄ§e

- Ø§Û.,Ø¹Ø±Ø´ÛŠ©
- Đ•Đ•Đ.Đ°Đ±ÑŠĐ»Đ³Đ°ÑĖÑ□Đ°Đ.
- Î•Î»Î»Î•Î½Î¹Î¹-
- Đ Ñ/Ñ□Ñ□Đ°Đ,Đ¹
- æ—Ÿææ-è²ž
- ä,æ-řç@ĉä½“
- ä,æ-řç¹□ä½“

Banknotes & Counterfeit Deterrence

Every country has legal restrictions on the reproduction of banknote images. The counterfeiting of currency is a crime, and while restrictions vary from

country to country, in some countries, any reproduction of banknote images " even for artistic or advertising uses " is strictly forbidden. Even in countries that allow some limited use of banknote images, there are specific rules and requirements. This website will provide you with information about reproducing banknote images and links to country-specific websites for further guidance.

While the overall economic losses to society from counterfeiting of currency are generally limited, the victims who suffer the most harm are individuals and businesses, because no one reimburses those who accept counterfeit notes. Counterfeit currency can also undermine confidence in the payment system, making the public uncertain about accepting cash for transactions.

The Central Bank Counterfeit Deterrence Group (CBCDGD) is responsible for this website. A counterfeit deterrence system (CDS) has been developed by the CBCDGD to deter the use of personal computers, digital imaging equipment, and software in the counterfeiting of banknotes. The CDS has been voluntarily adopted by hardware and software manufacturers, and prevents personal computers and digital imaging tools from capturing or reproducing the image of a protected banknote. The technology does not have the capacity to track the use of a personal computer or digital imaging tools.

For information specific to a particular country or the banknote image you want to use, click on the appropriate region on the map or select the relevant country or currency from the list.

1. Regions:

Select a region

Select a region from the list or click on the [map](#) below

[back to home](#)

Currency:

USD " US dollar; Federal Reserve notes

Official bank or department:

[U.S. Department of the Treasury](#)
[Bureau of Engraving and Printing](#)

Countries:

United States of America

Contact information:

Mrs Claudia Dickens
Department of the Treasury

[Bureau of Engraving and Printing](#)
14th and C Streets, SW
20228 Washington, DC
United States of America
Tel.: +1 202 874 3019

Languages:

English

Links:

[Reproduction rules](#)
[Images of Federal Reserve banknotes](#)

1. Latest queries

1. [AUD " Australian dollar](#)
2. [CAD " Canadian dollar](#)
3. [CHF " Swiss franc](#)
4. [DKK " Danish krone](#)
5. [EUR " euro](#)
6. [GBP " pound sterling](#)
7. [JPY " Japanese yen](#)
8. [NOK " Norwegian krone](#)
9. [SEK " Swedish krona](#)
10. [TRY " New Turkish lira](#)
11. [USD " US dollar](#)

General information about the reproduction of banknotes:

The Counterfeit Detection Act of 1992, Public Law 102-550, in Section 411 of Title 31 of the Code of Federal Regulations, permits color illustrations of U.S.

currency, provided that:

1. the illustration is of a size less than three-fourths or more than one and one-half, in linear dimension, of each part of the item illustrated;
2. the illustration is one-sided; and
3. all negatives, plates, positives, digitized storage medium, graphic files, magnetic medium, optical storage devices and any other thing used in the making of the illustration that contain an image of the illustration or any part thereof are destroyed and/or deleted or erased after their final use.

- [Press Releases](#)
- [FAQs](#)
- [Contact us](#)
-

Strahan Ted

From: Clarke Lenore
Sent: Monday, March 31, 2008 8:14 AM
To: Choy Edmund; Huynhtran Trucchi; Falat Ladislav; Hallock John; Humphrey V. Daniel; Cornell Dave; Curtis David; Strahan Ted
Subject: FW: tracking counterfeits

FYI

From: Daniel.A.Littman@clev.frb.org [mailto:Daniel.A.Littman@clev.frb.org]
Sent: Monday, March 31, 2008 7:30 AM
To: Daniel.A.Littman@clev.frb.org
Subject: tracking counterfeits

Tracking counterfeits through laser printers

David Canton

http://fpress.ca/newsstand/Business/Columnists/Canton_David/2008/03/31/5149061-sun.html

Though used for years, microscopic yellow tracking dots created by some colour laser printers have recently raised privacy concerns with the European Commission.

The European Commission is concerned printers that leave such a trail are breaking European laws. Franco Frattini, the EU Commissioner for Justice, Freedom and Security, said that "to the extent that individuals may be identified through material printed or copied using certain equipment; such processing may give rise to the violation of fundamental human rights, namely the right to privacy and private life. It might also be violating the right to protection of personal data."

Personal data is protected by the Data Protection Directive, but debate continues in Europe about how to define personal data. At times, it is uncertain what qualifies for protection.

Even if the information is not technically personal data, the tracking technology may still break the law. Article 7 of the Charter of Fundamental Rights of the European Union provides for the protection of private and family life, home and communication. Article 8 specifically protects personal data.

Printer makers are able to encode the serial number, manufacturing code and the date of printing through a series of small yellow dots interspersed on the printed paper. These dots are invisible to the naked eye.

This technology was developed nearly 20 years ago because laser-printing technology enabled counterfeiting. It was developed by printing companies in response to countries reluctance to sell laser printers without some means of tracing or tracking counterfeiters.

Recently, the Dutch railway police have been able to track counterfeits via printer serial numbers by tracking down the printer which was used to print fake tickets. A distributor in the Netherlands was visited by two police officers who knew the exact model of the printer used and hoped to learn the identity of the purchaser: As the company's records only revealed what batch the printer had arrived in,

12/18/2008

the police left with specific sales information about the entire batch: about 100 printers in all.

The Electronic Frontier Foundation -- online at www.eff.org -- has much information about the issue of secret printer dots.

They note, for example, that Xerox has admitted it provided tracking dots to government. At present, only select enforcement agencies have the capacity to read the codes. Though the agencies insist they only use the information gleaned for criminal counterfeit investigations, there are no laws to stop government from abusing the information.

It is also estimated that researchers are able to identify the model of printer used to create documents in 11 out of 12 models tested. However, to prove that a specific printer was used by counterfeiters, authorities would need the printer in question to confirm suspicions.

Printer owners can easily test whether their laser printers are printing yellow tracking dots on their documents by flashing a blue LED light on white parts of their document. If numerous black dots appear (yellow becomes black under a blue LED light) with a semblance of structure, it is likely the document contains tracking dots.

[REDACTED]
ATTORNEY AT LAW
[REDACTED]

NEW YORK, NEW YORK 10001

[REDACTED] November 30, 1995 [REDACTED]

Mr. Larry E. Roluff, Director
Bureau of Engraving and Printing
United States Department of the Treasury
14th and C Street, S.W. - Room 119 M
Washington, D.C. 20023

Re: Use of Electronic Scanning, Bar Coded Currency
and Databank Monitoring To Detect and Deter
Counterfeiting and Money Laundering

Dear Mr. Roluff:

Mr. William H. Pickle of the Secret Service has suggested that I might obtain from your office information as to the Advanced Counterfeit Deterrence Steering Committee's review of the use of bar code technology for possible inclusion in the comprehensive redesign of U.S. currency.

Mr. Pickle's suggestion was made in his November 13, 1995 letter to me (copy enclosed), which was a response to my October 25, 1995 letter to Secretary Rubin and the accompanying memorandum on the subject referenced above (copies enclosed).

As the correspondence with Secretary Rubin indicates, I am a consultant to CIAS, Inc., and to that extent I have a bias in favor of the work done in this field by the two CIAS inventors, [REDACTED] and [REDACTED].

But, beyond that, as a citizen I am convinced there is a real possibility that using modern bar coding and computer technology could be of great benefit to our Nation in dealing with the serious problems of counterfeiting and money laundering. At the very least, it merits in-depth study by the Treasury Department. Yet, apparently there has been no such study. Indeed, there has been institutional opposition to doing such a study.

Mr. Pickle refers to a review conducted by the ACD. But I surmise that the ACD's review of bar code technology was, at best, cursory. My belief is based partly on the fact that the ACD's review dealt with the "redesign" of the currency and, as such, would have been concerned with making it difficult or impossible to exactly copy the bills. While random number bar coding would complement that concern, the bar coding/databank approach is different in that it also provides for "accountability" -- in which

the authenticity of each individual bill can be validated by electronic scanning and comparison with a central databank. Also, I respectfully suggest, the bar code/databank approach offers overwhelming benefits for Government enforcement agencies which would have been clear if serious consideration had been given to that technology.

Even if I am correct in surmising that the ACD's review was very limited, we would like to be able to assess any points that were made; and, as you might guess, we would hope to have a further opportunity to try to interest the Secretary and your Bureau in doing a comprehensive study of the use of modern bar code and databank technology to detect and deter counterfeiting and money laundering.

In any event, following through on Mr. Pickle's suggestion, I respectfully request that your office provide us with "information on the specifics of the decision" by the ACD not to use bar coding. The specifics Mr. Pickle was referring to would presumably include information as to the factors which were the subject of the ACD's evaluations -- impact, proven reliability, durability, costs, public acceptance, and manufacturing limitations. We would, of course, reimburse the Bureau for copying and other costs involved.

Mr. Pickle's letter suggests that information with respect to some of the ACD's review might be classified. But I assume there would be no need for classification of information on what was probably the very limited review of bar coding technology. At that, classification would seem unnecessary where a negative decision was reached.

If, however, there is something in the ACD's decision about bar coding which is classified, it would be helpful if, in addition to receiving the non-classified parts of the ACD review and report, we could be given some general information about how extensive the review of bar code and databank technology was, in terms of pages in the report and the number of people and time involved in doing the studies.

I thank you for the consideration given this request.

Sincerely yours,


cc: Secretary Robert E. Rubin
William H. Pickle



DEPARTMENT OF THE TREASURY
UNITED STATES SECRET SERVICE

November 13, 1995

[REDACTED]
Attorney at Law
[REDACTED]

New York, New York 10001

Dear [REDACTED]

Your October 25, 1995, correspondence to Treasury Secretary Rubin has been forwarded to this office for a response. The United States Secret Service, as the agency responsible for the suppression of counterfeit United States currency is a member of the Advanced Counterfeit Deterrence Steering Committee (ACD). Other members include representatives from the Federal Reserve System, the Bureau of Engraving and Printing, and the Department of the Treasury.

The ACD Committee was actively involved in reviewing a variety of features which were in various stages of consideration, for inclusion in the comprehensive redesign of counterfeit currency. It is my understanding, that numerous overt and covert security features were evaluated based on several factors such as their impact, proven reliability, durability, public acceptance, manufacturing limitations, and production costs. The use of bar code technology was one of many features considered, but not adopted. Information on the specifics of the decision might be obtainable in an unclassified version from the Bureau of Engraving and Printing.

Your interest is appreciated.

Sincerely,

William H. Pickle
Executive Assistant
to the Director
(Congressional Affairs)

[REDACTED]
ATTORNEY AT LAW
[REDACTED]

NEW YORK, NEW YORK 10001

[REDACTED] October 25, 1995 [REDACTED]

Hon. Robert E. Rubin
Secretary of the Treasury
Office of the Secretary, Rm. 3330
Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D. C. 20220

Dear Secretary Rubin:

By way of reintroduction: I was general counsel of SCM Corporation and we met in 1985 when Goldman Sachs was helping us to defend against the Hanson takeover. You were a witness concerning the arbitragers' participation in the Hanson open market sweep; and you also priced the SCM/Merrill leveraged buyout debentures. All in all, even though the Second Circuit didn't agree with SCM's position, it was a noble defense effort.

I am writing to you about the use of electronic scanning, bar coded currency and databank monitoring to detect and deter counterfeiting, money laundering and other crimes.

Under the Crime Control Act of 1990, the Secretary of the Treasury in the prior Administration was required to conduct a study of electronic scanning of currency and to submit a report of the study to Congress by May 29, 1991. However, I understand the study was never made, and there was no report.

Ironically, the prior Administration's failure to do the electronic scanning study could reflect the kind of institutional resistance to technological change which Congressman Gingrich often complains about.

It could be that those with expertise in making bills impossible to exactly duplicate were reluctant to try a different approach emphasizing "accountability" -- in which the authenticity of each individual bill can be validated by electronic scanning and comparison with a central databank.

As indicated below, I recommend a Treasury study of the use of bar codes, electronic scanning and a databank for U.S. currency. However, it would seem that not much analysis is needed to see that on the simplest level the use of bar coding -- now so pervasive in the commercial world -- for our currency is long overdue. If nothing else, at a basic level, adding a degree of automation would give enhanced efficiencies in everyday operations

(sorting, counting, and recording) of Federal Reserve Bank Centers and all banks. Beyond that, in a situation where sophisticated counterfeiting has produced bills that cannot be spotted by tellers or sales clerks, an automatic bar code databank system would be a positive means to detect counterfeiting (including the daunting counterfeiting that is done to finance terrorists). The tracking capability of such a system, would also provide a powerful means of detecting money laundering and other crimes involving cash.

My interest in this subject stems from consulting work I have done for CIAS, Inc., which has developed and patented an electronic scanning/bar code/databank monitoring system to detect and deter counterfeiting, money laundering and other crimes.

In the past, [REDACTED], president of CIAS (and co-inventor of its binary coded binary bar code system), has had some contacts with officials in the Bureau of Engraving and Printing, the Secret Service and U.S. Customs. While there has been some interest in his work, the impetus for in-depth consideration of the system's possibilities was not there.

A request by the Secretary of the Treasury for a study of possible use of electronic scanning of bar coded currency would provide the impetus for serious consideration of recent technological developments in this area, with inputs from experts on coding, symbology, scanning systems and computer data base monitoring.

I enclose a short memorandum which reviews the provisions in the Crime Control Act of 1990 for an electronic scanning study and discusses reasons why apparently no study was made. The memorandum recommends a similar but less formal study which might be done in two months.

If there is a Treasury study, or if there is any other interest on the part of Treasury officials, I, Mr. Storch and others from CIAS would be pleased to meet with the officials to discuss the use of a bar coding system in the battle against counterfeiting, money laundering, terrorism, and other crimes.

Very truly yours,
[REDACTED]

October 25, 1995

MEMORANDUM

For: United States Department of the Treasury

By: [REDACTED]
Consultant to CIAS, Inc.

Subject: Use of Electronic Scanning, Bar Coded Currency
and Databank Monitoring To Detect and Deter
Counterfeiting, Money Laundering and Other Crimes

This Memorandum is submitted in support of the recommendation that the Treasury Department conduct a study of the above subject.

A study of this subject was mandated in the Crime Control Act of 1990. But it is my understanding that the prior Administration did not carry out the mandate, and the study was never done.

Whatever the reasons for the prior Administration's failure to do the mandated study and report in 1991, consideration should now be given to the possibilities for using electronic scanning technology in a new databank "accountability" approach to deterrence of counterfeiting and money laundering.

The magnitude of the counterfeiting and money laundering problems is such that any reasonable possibility for obtaining improved results in dealing with those problems should be thoroughly investigated and analyzed.

This Memorandum will give a summary of the study which was outlined in the Crime Control Act of 1990, and it will include a short discussion of the reasons no study was made. In support of the idea that a study is desirable now, the Memorandum describes

the CIAS system as being the kind of approach which would be worthy of consideration in a study of the use of electronic scanning to aid law enforcement efforts.

1. The Crime Control Act of 1990

A copy of the Crime Control Act of 1990, Public Law 101-647, November 29, 1990, 101st Congress, 104 STAT. 4789, is attached to this Memorandum. "Title I - International Money Laundering" included "Section 102 - Electronic Scanning Of Certain United States Currency Notes," (other sections dealt with Currency Transaction Reports and some technical amendments to other money laundering statutes).

a. The mandated study of electronic scanning

Under Subsection 102 (a), the Secretary of the Treasury was to appoint an Electronic Scanning Task Force to:

(A) study methods of printing on U.S. currency notes of \$10 or more an individual serial number that could be read by electronic scanning;

(B) assess costs of implementing such electronic scanning of currency notes; and

(C) make recommendations as to the amount of time needed to implement such electronic scanning.

Under Subsection 102 (b), the Secretary of the Treasury was to issue a report to Congress by May 29, 1991 which summarized the findings and recommendations of the Task Force and included any additional recommendations by the Secretary.

b. The failure to do the mandated study

In December 1994, Leonard Storch, president of CIAS, Inc., was advised by Thomas Ferguson, of the Bureau of Engraving & Printing, that the Department of the Treasury had not done the 1991 study and report. He referred to a typographical error in the statute which apparently made it unworkable.

The problem was that under 102 (a)(2), the Electronic Scanning Task Force had to include: (A) the Assistant Secretary for Enforcement, (B) experts from five scanning technology fields, and (C) representatives of the Bureau of Engraving, the Federal Reserve and the Secret Service. But 102 (a)(3) stated that "Except as provided in paragraph (2)(A), no individual who is a full-time employee of the Federal government may serve as a member of the Task Force." The typographical error is that obviously the exceptions in 102 (a)(3) should have included (2)(A) and (2)(C).

Of course, even accepting the typographical error as it was, the Secretary could have appointed Federal Representatives who were consultants to but not full-time employees of the three agencies designated in (2)(C). At the same time he could also have had three full-time experts from those agencies (whose input Congress obviously wanted) participate in the study even though they were not formally members of the Task Force.

It would seem that the problem of the typographical error in the statute could have been resolved if, in 1991, there had been real interest in the Department in doing the electronic scanning study. Without such interest and with likely opposition from some

experts in the Department who were committed to more traditional approaches to fighting counterfeiting, the typo excuse carried the day; and apparently Congressional interest lagged and died.

2. Recommendation for a New Electronic Scanning Study

It is respectfully submitted that a study of the possible use of electronic scanning of individual U.S. currency notes was a good idea in 1990 and the desirability of such a study is even greater today.

(a) The desirability of a study of possible use of electronic scanning technology

To say the least, counterfeiting and money laundering continue to be serious problems. The seriousness of the problems can be seen in the calls for a "war on drugs" and the related call for a "war on drug money" by Rachel Ehrenfeld and others; and it can be seen in the references during the last month in New York City newspapers to an "avalanche" and a "flood" of counterfeit money and to the use of "supernotes" as "economic terrorism" under the possible sponsorship of Middle Eastern governments (a subject which has received considerable attention from the House Republican Research Committee on Terrorism and Unconventional War).

The use of the word "war" is appropriate; and, as in wartime, our Government's response ought to be to expedite the mobilization of every possible means of fighting the war, including researching all possible new ways of achieving victories which have eluded us in the past. Given the billions that have been

spent and are being spent in these wars, without great successes (a March 1993 ABA Journal article said that during the years of the Bush administration, federal, state and local governments spent about \$100 billion in the war on drugs) and the additional billions of losses incurred by society, even if use of an electronic scanning bar code system were very costly (which would not have to be the case), the money would be well spent if it were to produce positive results.

The new \$100 bills are an impressive response to the mounting counterfeiting problem. But this traditional approach in dealing with counterfeiting -- making notes that are impossible to exactly duplicate -- has become progressively harder to implement because of sophisticated technology which is available for use by well financed counterfeiting interests. At that, even if bills cannot be exactly duplicated, minute differences between genuine bills and some of today's counterfeits cannot readily be detected by lay persons.

Pertinent in these circumstances are the admonitions of Vice President Gore and Speaker Gingrich to the effect that our Government should be more open to the use of modern technologies.

Electronic scanning and related technologies are certainly among the technologies whose uses in recent years have expanded exponentially: bar coding is universally used in all phases of commerce, including manufacturing, distribution, wholesaling and retailing; retailers, whatever the size, are connected to electronic credit card reading facilities; ATM's are available for

instantaneous use nationally and internationally; and huge computer databases are in use as computer capacity increases toward infinity and computer costs go down.

As indicated in the discussion of the CIAS system below, use of electronic scanning technology would bring an added new approach to bear on the counterfeiting problem. In addition to the Treasury's present improved techniques for making notes impossible to copy exactly, an electronic scanning and databank approach would provide accountability: scanning individually coded notes the authenticity of which could be verified by electronic reference to a databank.

Not only would the electronic scanning approach be an added new tool to fight counterfeiting, it could provide significant breakthroughs in combatting money laundering and other crimes.

(b) Suggestions for a study format

The subjects of the study outlined in the 1990 Act are still good ones -- dealing with (a) methods for use of electronic scanning, (b) costs, and (c) estimates of the time it would take to implement such an approach. Essentially, the study would involve analyses of the feasibility of an electronic scanning approach, but it would also need to include practical assessments of exactly how such an approach would add to Enforcement's ability to detect and deter counterfeiting, money laundering and other crimes.

The study itself could be quite informal; it could be done by a relatively few people in the Department. It would not be necessary or desirable to have a formal Task Force like that pro-

vided for in the 1990 Act. But the study should still have inputs from agencies and disciplines such as those listed in the Act -- persons from Enforcement, the BEP, the Secret Service, the Federal Reserve, as well as the U.S. Customs, FBI, CIA and DEA, and experts in bar coding, printing, symbology, scanning systems, computer data compilation, large computer databank installations, and computer software.

It would be best to avoid large committee meetings; and individual interviews of and written submissions by experts would be preferable to a "hearings" type of approach. Ideally, specific responsibilities could be assigned to a relatively few persons who would be working full-time on the study. One person could be a coordinator, expediter and supervisor; and it might be helpful to have that person assisted by one individual who would be a champion of the electronic scanning approach and by another who would function as devil's advocate. Lastly, wartime "impossible" schedules could be set with the goal of having the analyses and a report ready for the Secretary within two months.

End of suggestions.

3. A Summary Description of the Use of an Electronic Scanning System To Detect and Deter Counterfeiting and Money Laundering -- The CIAS Scanning/Bar Code/Databank System

The CIAS system is covered by two patents, U.S. Patent Nos. 4,814,589 and 5,283,422 and a pending patent application. The following is a description of various elements in the system.

(a) The BCB currency bar code

It is already true that each U.S. currency note has its own unique identification, including a serial number. If it is thus desirable to have such I.D. serial numbers, then, just at that simple level, bar coded I.D. serial numbers would have to be an improvement. Optical Character Reading ("OCR") devices can be used to read printed numbers; but in terms of cost, size and accuracy, the OCR devices are not practical and are markedly inferior to bar code scanning devices. Without getting into sophisticated aspects of a bar code system, bar code scanning would add substantial efficiencies in everyday bill handling, sorting, counting and record keeping operations -- just as bar codes have done in thousands of other applications.

The capacity of the suggested format of the CIAS binary coded binary ("BCB") bar code would allow for greater than 9,000,000,000,000,000 (9×10^{15}) unique currency serial numbers -- more numbers than would be needed for all of the World's currencies. This BCB format would be 1.41 inches long by .25 inches high (smaller than most existing bar code symbology), with the narrowest line of the code being .01 inch in width. Exhibit A to this Memorandum is an example of a format for using the BCB bar code on twenty dollar bills.

The BCB bar code is unique. BCB has the strongest inherent error control capability of any existing bar codes, and it is the only linear bar code with error correcting. Moreover, BCB is the only modern bar code that has been designed so that it can

be printed with currency numbering machines just as serial numbers are printed.

(b) Scanning and databank detection of counterfeit currency

The CIAS system would use a central currency databank to track and record information about currency transactions. When a bill is issued, its coded I.D. serial number would be recorded in the databank, along with distribution information. As the system is phased in, information could be recorded in the databank to reflect banking deposits and withdrawals, and large retailer transactions.

Using the CIAS system and databank, the Federal Reserve could initially scan the currency it received from the banks to see if any I.D. serial numbers are in a crime "hot" list (e.g., planted "tracer" currency or stolen currency); and, then, a more comprehensive use of the databank would involve the determination of whether the scanned currency I.D. serial numbers are authentic or whether a seemingly authentic I.D. serial number is already accounted for elsewhere or is otherwise part of a pattern of duplicate numbers. Computerized statistical analyses and following "paper trails" could also identify counterfeit bills or other illegal cash and the banks from which it comes.

(c) Security I.D. numbers

To provide a further precaution against counterfeits, the BCB bar code has the capability for using random digits as part of the serially printed coded numbers. Thus, one more bar coded digit

can be added to a bill's bar coded serial I.D. number; the digit is not serially selected, but is randomly selected and goes into the databank with the I.D. serial number of the bill.

The added digit would be checked automatically in the central databank when a bill is scanned; if the digit is not the same as the randomly selected digit which was originally stored, the bill is counterfeit. Thus, even if a counterfeiter were able to serially print bar coded numbers, he could not predict what the randomly selected digit would be -- and that would be another deterrent to large scale counterfeiting.

(d) Practical considerations

After first bar coding the currency I.D. serial numbers on the bank notes, there would be the large practical problem of implementing the system by putting the central databank on line. No doubt, concern about this underlay the 1990 Act's requirements for studying costs and the estimated time to implement a system. But in recent years scanning devices have come into use in all fields with increased effectiveness and at decreased cost. Also, monumental strides have been made in computerizing all aspects of the banking business. All in all, it would seem that there would be no shortage of contractors eager to work out solutions to databank implementation problems.

The initial phase of implementing the system might only involve use of limited sampling scanning and monitoring by enforcement agencies and the Federal Reserve Bank Centers. But as banks were charged back by the Federal Reserve for bad bills received

from them, the banks would have an incentive to install scanners and become part of the databank system; and, as casinos were charged back by the banks for bad bills received from the casinos, the casinos would have an incentive to install scanners and become part of the databank system; and large retailers would be similarly motivated.

The advantages of this automatic accountability system should be obvious to bankers and others. Among other things, they would not have to rely on the ability of a teller or retail clerk to spot the minute imperfections which characterize some of the notes produced by well financed and equipped counterfeiting operations like those reportedly located in Lebanon, Syria, Iran and Columbia.

(e) Money laundering and CTR's

Standard anti-counterfeiting measures -- making the notes impossible to exactly duplicate -- are not directly involved with the problem of money laundering. But a tracking system such as the CIAS system could be of great help in dealing with that problem. Just judging from the statute, it would appear that it was concern about money laundering which stimulated the mandate for a study of electronic scanning in the 1990 Crime Control Act.

Right on point was a Reader's Digest (April 1990) review of Claire Sterling's book "Octopus" which concluded that "a data bank to track large currency transactions" was desperately needed to fight crime. Similarly, former Attorney General Thornburgh said that "the most vulnerable point for any drug operation is the door-

way to the bank." The problem is immense; one estimate, given on Nightline, December 6, 1989, was that 26 million pounds of twenty dollar bills were laundered annually.

The tracking capability of the CIAS system would greatly add to Law Enforcement's ability to detect money laundering.

For example, in the past, Cash Transaction Reports ("CTRs") (also a subject of the 1990 Act) of transactions over \$10,000 have been used in the fight against money laundering, apparently with limited success. Presently only a small percentage of the manually filled out and processed CTRs can be checked, and those that do get examined may often have inaccurate or incomplete information. But the inevitable involvement of local banks with the bar code currency databank system could mean that CTRs would be replaced with more useful automatically generated information. Also there could be less reliance on bankers reporting suspicious transactions and more reliance on computer analyses of tracking patterns.

An electronic CTR system would have the ability to check for "traced currency", such as planted drug money, stolen money or terrorist money. This could, for example, lead to significant victories in the war on drugs -- victories which would be won with brains, not brawn.

(e) Terrorism

It could be expected that as the currency databank grows, software would be developed to enable authorities to deal with crime more effectively -- e.g., tracking terrorist activities through their currency transactions. But even without such

sophistication, the bar code currency databank system would help in the fight against terrorism simply by depriving terrorists of their financing, which, reportedly, often involves the use of counterfeit money -- and, as discussed above, the system would provide a means of counterfeit detection and deterrence which has not heretofore been available.

Conclusion

It is respectfully submitted that the Department of the Treasury should conduct a study of systems using electronic scanning, individually bar coded currency notes, and databank monitoring to detect and deter counterfeiting, money laundering, and other crimes.

Such a study would be a demonstration that the Treasury Department is, as it should be, open to exploring the possibilities for applying today's technologies to add to its traditional methods of fighting counterfeiting. Moreover, if, as a result of the study, the possibilities for using a new databank accountability approach to the counterfeiting problem were to become realities, the realities would also include use of the system to win some much needed victories in the war against drugs and other crimes.

RS

Below is a sample, shown at 75% of actual size, of what bar coded currency might look like:

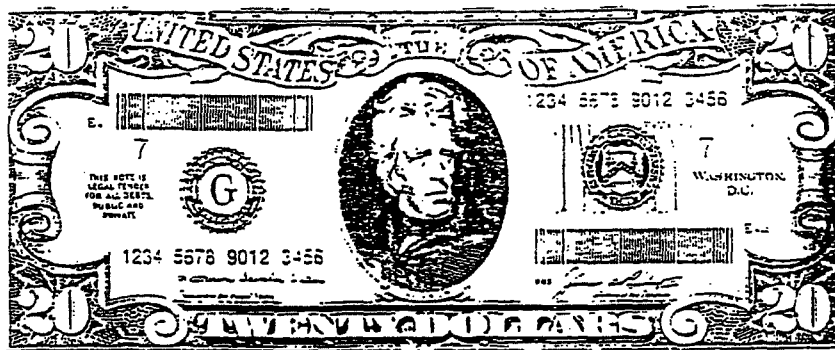


EXHIBIT A
Memorandum
10/25/95

Public Law 101-647
101st Congress

An Act

To control crime.

Nov. 29, 1990

[S. 3266]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Crime Control
Act of 1990.
18 USC 1 note.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Crime Control Act of 1990".

**TITLE I—INTERNATIONAL MONEY
LAUNDERING**

SEC. 101. REPORTS ON USES MADE OF CURRENCY TRANSACTION RE-
PORTS.

31 USC 5311
note.

Not later than 180 days after the effective date of this section, and every 2 years for 4 years, the Secretary of the Treasury shall report to the Congress the following:

(1) the number of each type of report filed pursuant to subchapter II of chapter 53 of title 31, United States Code (or regulations promulgated thereunder) in the previous fiscal year;

(2) the number of reports filed pursuant to section 6050I of the Internal Revenue Code of 1986 (regarding transactions involving currency) in the previous fiscal year;

(3) an estimate of the rate of compliance with the reporting requirements by persons required to file the reports referred to in paragraphs (1) and (2);

(4) the manner in which the Department of the Treasury and other agencies of the United States collect, organize, analyze and use the reports referred to in paragraphs (1) and (2) to support investigations and prosecutions of (A) violations of the criminal laws of the United States, (B) violations of the laws of foreign countries, and (C) civil enforcement of the laws of the United States including the provisions regarding asset forfeiture;

(5) a summary of sanctions imposed in the previous fiscal year against persons who failed to comply with the reporting requirements referred to in paragraphs (1) and (2), and other steps taken to ensure maximum compliance;

(6) a summary of criminal indictments filed in the previous fiscal year which resulted, in large part, from investigations initiated by analysis of the reports referred to in paragraphs (1) and (2); and

(7) a summary of criminal indictments filed in the previous fiscal year which resulted, in large part, from investigations initiated by information regarding suspicious financial transactions provided voluntarily by financial institutions.

SEC. 102. ELECTRONIC SCANNING OF CERTAIN UNITED STATES CURRENCY NOTES.

(a) ELECTRONIC SCANNING TASK FORCE.—(1) Not more than thirty days after the date of enactment of this section, the Secretary of the Treasury (hereafter in this section referred to as the "Secretary") shall appoint an Electronic Scanning Task Force (hereafter in this section referred to as the "Task Force") to—

(A) study methods of printing on United States currency notes issued under section 51115 of title 31, United States Code, in denominations of \$10 or more a serial number on each such United States currency note that may be read by electronic scanning;

(B) make an assessment of the cost of implementing such electronic scanning of such United States currency notes; and

(C) make recommendations about the amount of time needed to implement such electronic scanning.

(2) In appointing members to the Task Force described in subsection (a), the Secretary shall appoint such number of members as the Secretary determines to be appropriate. The Secretary, shall, at a minimum appoint to the Task Force—

(A) the Assistant Secretary for Enforcement in the Department of the Treasury (who shall serve as a nonvoting, ex officio member);

(B) at least one recognized expert from each of the following fields relating to electronic scanning technology:

(i) coding,

(ii) symbology,

(iii) scanning systems,

(iv) computer data compilation, and

(v) printing technology, and

(C) Representatives from each of the following:

(i) the Bureau of Engraving and Printing,

(ii) the Federal Reserve Board, and

(iii) the United States Secret Service.

(3) Except as provided in paragraph (2)(A), no individual who is a full-time employee of the Federal Government may serve as a member of the Task Force.

(4) The provisions of the Federal Advisory Committee Act shall not apply with respect to the Task Force.

(5) Members of the Task Force shall, while attending meetings and conferences of the Task Force or otherwise engaging in the business of the Task Force (including travel time), be entitled to receive compensation at a rate fixed by the Secretary, but not exceeding the rate specified at the time of such service under GS-18 of the General Schedule established under section 5332 of title 5, United States Code.

(6) While away from their homes or regular places of business on the business of the Task Force, such members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by section 5703 of title 5, United States Code, for persons employed intermittently in the Government service.

(7) Upon the issuance of the report by the Secretary under subsection (b), the Task Force shall cease to exist.

(b) REPORT TO THE CONGRESS.—Not later than one hundred and eighty days after the date of enactment of this section, the Secretary shall issue a report to the appropriate committees of the Congress

that summarizes the findings and recommendations of the Task Force under subsection (a)(1), and includes any additional recommendations by the Secretary.

(c) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out the purposes of this section.

SEC. 103. CONFORMING AMENDMENT RELATING TO THE EQUITABLE TRANSFER OF FORFEITED PROPERTY TO A PARTICIPATING FOREIGN NATION.

Section 981(i) of title 18, United States Code, is amended—

(1) by striking out the matter before paragraph (1);

(2) by realigning paragraphs (1) through (5) 2 ems to the left, so that the left margins of such paragraphs are flush;

(3) by striking out “(1) Notwithstanding” in paragraph (1) and all that follows through the end of the second sentence of that paragraph and inserting in lieu thereof the following:

“(i)(1) Whenever property is civilly or criminally forfeited under this chapter, the Attorney General or the Secretary of the Treasury, as the case may be, may transfer the forfeited personal property or the proceeds of the sale of any forfeited personal or real property to any foreign country which participated directly or indirectly in the seizure or forfeiture of the property, if such a transfer—

“(A) has been agreed to by the Secretary of State;

“(B) is authorized in an international agreement between the United States and the foreign country; and

“(C) is made to a country which, if applicable, has been certified under section 481(h) of the Foreign Assistance Act of 1961.”;

(4) by inserting after “Attorney General” in the third and fifth sentences of paragraph (1) the following: “or the Secretary of the Treasury”; and

(5) by striking out the last sentence of paragraph (1).

SEC. 104. ADDITION OF CONFORMING PREDICATE MONEY LAUNDERING REFERENCES TO “INSIDER” EXEMPTION FROM THE RIGHT TO FINANCIAL PRIVACY ACT.

Section 1113(1)(2) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3413(1)(2)) is amended by inserting “or of section 1956 or 1957 of title 18, United States Code” after “any provision of subchapter II of chapter 53 of title 31, United States Code”.

SEC. 105. CLARIFICATION OF DEFINITION OF “MONETARY INSTRUMENTS”.

Section 1956(c)(5) of title 18, United States Code, is amended to read as follows:

“(5) the term ‘monetary instruments’ means (i) coin or currency of the United States or of any other country, travelers’ checks, personal checks, bank checks, and money orders, or (ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery;”.

SEC. 106. MONEY LAUNDERING AMENDMENTS.

Section 1956(c)(1) of title 18, United States Code, is amended by striking “State or Federal” and inserting “State, Federal, or foreign”.

SEC. 107. CORRECTION OF ERRONEOUS PREDICATE OFFENSE REFERENCE UNDER 18 U.S.C. 1956.

Section 1956(c)(7)(D) of title 18, United States Code, is amended by striking out "section 310 of the Controlled Substances Act (21 U.S.C. 830) (relating to precursor and essential chemicals)" and inserting in lieu thereof "a felony violation of the Chemical Diversion and Trafficking Act of 1988 (relating to precursor and essential chemicals)".

SEC. 108. KNOWLEDGE REQUIREMENT FOR INTERNATIONAL MONEY LAUNDERING.

Section 1956(a) of title 18, United States Code, is amended—

(1) in paragraph (2) by inserting at the end the following: "For the purpose of the offense described in subparagraph (B), the defendant's knowledge may be established by proof that a law enforcement officer represented the matter specified in subparagraph (B) as true, and the defendant's subsequent statements or actions indicate that the defendant believed such representations to be true."; and

(2) in paragraph (3) by striking "For purposes of this paragraph" and inserting "For purposes of this paragraph and paragraph (2)".

BANK FOR INTERNATIONAL SETTLEMENTS, BASLE/SWITZERLAND

TELEFAX TRANSMITTAL COVER SHEET

Transmission priority: regular

File:
03-31-87

Date: 3rd June 98

Number of pages (including cover sheet): 18

To:

Fax No: (43 1) 404 15 98
OESTERREICHISCHE NATIONALBANK
For the attention of: [REDACTED], Technical Manager

Fax No: (32 2) 221 31 09
BANQUE NATIONALE DE BELGIQUE
For the attention of: [REDACTED] Chef du Département de l'Imprimerie

Fax No: (1 613) 782 77 07
BANK OF CANADA
For the attention of: [REDACTED] Department of Banking
Operations

Fax No: (420 2) 24 21 88 14
CZECH NATIONAL BANK, STATE PRINTING WORKS ON SECURITIES
For the attention of: [REDACTED] Technical Manager

Fax No: (45 33) 63 71 21
DANMARKS NATIONALBANK
For the attention of: [REDACTED] Director, Banknote Printing Works

Fax No: (358 9) 891 887
SETEC OY, Vantaa, Finland
For the attention of: [REDACTED]

Fax No: (33 1) 42 92 30 09
BANQUE DE FRANCE
For the attention of: [REDACTED] Directeur Général de la Fabrication
des Billets

Fax No: (49 69) 95 66 32 89
DEUTSCHE BUNDESBANK
For the attention of: [REDACTED], Leiter der Hauptabteilung Hauptkasse

To: Fax No: (30 1) 67 25 977
BANK OF GREECE, BANKNOTE PRINTING WORKS
For the attention of: [REDACTED]

If this transmission is not complete, please call (41) 61/280 85 85

B.I.S., Basle, Switzerland

Telefax numbers: (41) 61/280 91 00

(41) 61/280 81 00

Telex number: 962487

Telephone number: (41) 61/280 80 80

Transmitted by
(For internal use only)

03.06.1998 16:16

BANK FOR INTERNATIONAL SETTLEMENTS, BASLE/SWITZERLAND

TELEFAX TRANSMITTAL COVER SHEET

Fax No: (36 1) 332 05 93
HUNGARIAN BANKNOTE PRINTING CORPORATION
For the attention of: [REDACTED] General Manager

Fax No: (353 1) 296 65 36
CENTRAL BANK OF IRELAND
For the attention of: [REDACTED], Assistant Director General

Fax No: (39 6) 47 92 76 74
BANCA d'ITALIA
For the attention of: [REDACTED], Condirettore Centrale
Capo del Servizio Fabbricazione Carte Valori

Fax No: (81 3) 52 03 73 07
THE BANK OF JAPAN
For the attention of: [REDACTED] Director, Issue Department

Fax No: (31 20) 524 25 26
DE NEDERLANDSCHE BANK
For the attention of: [REDACTED], Deputy Director Sector
Payments

Fax No: (47 22) 31 66 58
NORGES BANK SEDELTRYKKERI, Oslo
For the attention of: [REDACTED] Director

Fax No: (351) 63 851 304
BANCO DE PORTUGAL
For the attention of: [REDACTED] Deputy Manager - Currency Issue
Dpt.

Fax No: (34 91) 504 2943
FABRICA NACIONAL DE MONEDA Y TIMBRE, Madrid
For the attention of: [REDACTED]

Fax No: (41 31) 327 02 21
SCHWEIZERISCHE NATIONALBANK
For the attention of: [REDACTED] Direktor, Bereich Bargeld

Fax No: (90 312) 324 34 30
CENTRAL BANK OF THE REPUBLIC OF TURKEY
For the attention of: [REDACTED] Vice Governor

To: Fax No: (44 181) 502 10 07
BANK OF ENGLAND
For the attention of: [REDACTED] General Manager

If this transmission is not complete, please call (41) 61/280 85 85

U.I.B., Basle, Switzerland

Telefax numbers: (41) 61/280 91 00

(41) 61/280 81 00

Telex number: 962487
Telephone number: (41) 61/280 80 80

Transmitted by
(for internal use only)

BANK FOR INTERNATIONAL SETTLEMENTS, BASLE/SWITZERLAND

TELEFAX TRANSMITTAL COVER SHEET

Bank of England Printing Works

Fax No: [REDACTED]
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
For the attention of: [REDACTED]
Assistant to the Board for Federal Reserve System
Affairs
Office of Board Members

Fax No: [REDACTED]
AB TUMBA BRUK
For the attention of: [REDACTED] Director

Fax No: (44 181) 532 09 33
BANK OF ENGLAND PRINTING WORKS
For the attention of: [REDACTED] Chief Scientist

Fax No: (1 202) 874 34 83
BUREAU OF ENGRAVING AND PRINTING, DEPARTMENT OF THE TREASURY
For the attention of: Mr. Robert Stone

From: [REDACTED]
Secretary SSG-2
Coordinating Services for Central Banks and International Organisations

Ref./Comments:

On behalf of the Chairman, please find attached the following documents for the meeting of SSG-2 on 12th June:

- 1. Agenda.
- 2. Summary of SSG-2 activities.
- 3. Digimarc agreement.
- 4. Appendices A-D.

I look forward to meeting you in Stockholm.

Kind regards,

[REDACTED]

If this transmission is not complete, please call [REDACTED]

B.I.S., Basle, Switzerland

Telefax numbers: (41) 61/280 91 00

(41) 61/280 81 00

Telex number: 962487
Telephone number: (41) 61/280 80 80

Transmitted by
(For internal use only)

1/6/98

AGENDA
Plenary SSG-2 Meeting
Stockholm - 12 June 1998

- 09:00** Opening Remarks/Introductions
Status Report on Computer Systems
Initial Survey & Discussions
Progress with Digimarc
Agreement for α -phase prototype
- 09:30** Digimarc Presentation/Demonstration
- 10:30** Break
- 11:00** Discussion with Digimarc (Questions/Answers)
- 11:30** Discussion on Computer Systems
Reactions from Delegates on Digimarc Presentation
SSG-2 Interface with Other Organizations
Schedule/Actions/Future Decisions
- 12:30** SSG-2 Membership Status
Revised Financial Model/Funding Allocation
1998-1999 Budget and Work Plan
- 13:00** Lunch
- 14:30** Discussion on Financial Model/Budget/Work Plan
- 15:30** Status Financial Account
Status of Common Mark System - Implementation/Licencing
Status of Checking System
Status of Pressroom System
Status of Bekaert/Arjo-Wiggins System
Status of Tracing System
- 16:00** Future Meetings
- Steering Committee - 29 October 1998 at BIS (tentative)
- Steering Committee - 26 January 1999 at BIS (review Digimarc results)
- All sponsors - 16 February 1999 at BIS (decision on Digimarc)
- 16:30** Any Other Business/Depart

T41 01 220 1000 D10 - DKA D12
00041 01 200 2100 D.1.3. BASEL

SUMMARY OF SSG-2 ACTIVITIES

June 1996 - May 1998

The SSG-2 has been engaged in four initiatives. Banknote recognition by color laser copiers using Common Marks, and banknote recognition by computer systems using Digital Watermarks have been the primary focus of the work.

1. Color Laser Copiers (Common Marks)

After successfully completing the testing of the Common Mark recognition system in copiers, a Memorandum of Understanding with the JBMA was signed to incorporate the detectors in all new production lines of color laser copiers which started production after January 1, 1997. Installation of the detectors is now underway in color laser copiers from all major copier manufacturers. In addition to the Common Mark (SC1) for SSG-2 sponsoring countries, a different Common Mark (SC2) was developed and made available to non-SSG2 countries for "licence fees" paid to the SSG-2 through the B.I.S. A total of 8 non-SSG2 countries have licenced the SC2 Common Mark.

The latest version of the Checking System Software from Omron had some initial difficulties, but these are being addressed and an improved version of the Manual is being sent out to users.

2. Press Room Unit

Omron has also provided a quote for a unit which could be used as a Quality Control Check on the Common Marks in the Press Room. The unit would be a color copier, modified to provide output as to the number and type of marks detected. This would be produced by Omron if there is sufficient demand for it, and assuming 20 units are sold, cost would be 5,000,000 Yen. Although a questionnaire will be circulated shortly to all Heads of Delegation to determine the extent of any interest in a Press Room unit, it would be helpful if Heads of Delegation could provide preliminary information on any interest at the 12 June meeting in Stockholm.

3. Bekaert System

Although the use of steel fibers in paper was initially rejected by the JBMA as being unsuitable for banknote detection by copiers, a new technique has been proposed by Bekaert and Arjo-Wiggins (in conjunction with PA Technology). This new technique involves the use of special low coercivity magnetic steel fibers in paper. The fibers are detected by a simple radio frequency technique. Although the SSG-2 is cooperating with this development, the viability of this technique for copiers remains to be demonstrated.

by Bekaert to the SSG-2 and the JBMA.

4. Tracing System

The Tracing System has proved to be a success with a number of Police Forces around the world in solving crimes or convicting counterfeiters. An up-dated version of the BITMAP ANALYSIS software is now available from the JBMA. The JBMA has requested payment of 500,000Yen for this software up-grade to cover a portion of the development costs. The up-grade includes new manuals and listings of copiers models. Copier manufacturers will continue to provide assistance in identifying specific copiers at no additional cost.

5. Computer Systems (Digital Watermarks)

Following a period of research and discussion, the SSG-2 has embarked on a program to develop banknote detection for use in computer systems. The system is based on the ideas behind the Digital Watermarking techniques used in computer graphics to protect the copyright of images. An initial feasibility study was successfully performed for the SSG-2 by Digimarc, a leading U.S. company in the field. They have now been engaged to work with the SSG-2 on development and testing of an Alpha prototype for consideration by the Steering Committee in early 1999. If this effort is successful, it will be necessary to agree with Digimarc and the computer industry upon a strategy for implementation into computer systems. Any agreements may include software, scanner, printer and computer manufacturers.

The SSG-2 anticipates a number of options may be available for response to recognition of a banknote by the computer system. For example, alteration of the digital data file, alteration of any printed output, and display of a warning are three potential responses. The possible responses may have differing legal implications within the sponsoring countries. A questionnaire will be distributed to Heads of Delegation in the near future to identify possible legal issues on the response of computer systems to banknote recognition.

Although extensive testing must be completed, the modified digital watermark (to be called a DR marc and standing for document recognition mark, but already known colloquially as "Doctor marc") is expected to be designed to have only a very small effect on banknote designs.

6. Another meeting of all sponsoring countries has been scheduled for 16 February 1999. This meeting will be held at the BIS to decide whether the SSG-2 should continue toward implementation of the Digimarc system.

SSG-2 PLENARY GROUP MEETING, 12 JUNE, STOCKHOLM**Outline Work Plan****1 Digimarc Programme (Alpha Phase)****1.1 Meetings:**

- (a) **July 9/10 1998, Haarlem**
Meeting with Digimarc
- (b) **August 27/28 1998, Portland**
Progress Meeting with Digimarc
- (c) **October 8/9 1998, Portland**
Progress Meeting with Digimarc
- (d) **November/December 1998, Portland (?)**
Final Meeting with Digimarc, Alpha Phase
- (e) **January 1999**
SSG-2 for Report on Alpha Phase to SSG-2 Steering Committee and Recommendations.

Supplementary meetings are envisaged for meeting with Software Companies, Computer Industry companies in October/November 1998. An attempt will be made to arrange these at the same times as the above meetings if possible.

1.2 Test Work

- (a) Algorithmic Print Testing* (early July)
- (b) Controlled Parameter Print Testing* (early September)
- (c) Production Print Testing* (end October/early November)
- (d) Adversarial Analysis* (September-November)
- (e) Discussion with Beta customers (November 1998)
- (f) Possible sample testing for Intaglio/Paper DR Marks

* Possible costs to SSG-2

2 DRmarc - Future Work Programme (Beta Phase)

- (a) Progress meetings with Digimarc (say total 3)
- (b) Visits to Beta customers (say 2)
It is possible that (a) and (b) can be combined.
- (c) Visits to Software/Hardware Companies (3?)
- (d) Adversarial Analysis

3 **Other Work**

3.1 It may be necessary to visit Tokyo to view a demonstration of Bekaert system. Other topics which may need discussion are Tracing System, Common Marks PR Unit, interaction of DRmarc with Common Marks etc.

3.2 Steering Committee Meetings 'Policy' (Toronto) Group meetings will probably be required during the next 12 months.



Chairman, SSG-2 Working Group

STATEMENT OF ACCOUNTS for TWO YEARS ENDING 31.05.98

	£
Opening Balance (A) as at 01.06.96	402,843.63
<u>Income:</u>	
Subscriptions*	243,153.00
SC2 Licences	43,843.56
Interest	35,356.79
Expenses Repaid	257.05
TOTAL INCOME (B)	<u>322,510.40</u>
* Three subscriptions not included one of which is in course of payment	
<u>Expenditure:</u>	
Travel (and related expenditure)	211,387.30
Research & Testing**	333,166.65
TOTAL EXPENDITURE (C)	<u>544,553.95</u>
** includes payment of \$500,000 to Digimarc	
Balance of Income/Expenditure [D=(B-C)]	-222,043.55
Cash at Bank as at 1.6.98 [= A+D] =	180,800.08
Estimated Outstanding Travel Costs and Research Liabilities =	-45,000.00
Subscriptions for 1997/98 (not included above)	29,000.00
Estimated Balance Currently Available =	164,800.00

1. **Definitions**

The following terms, when used in this Agreement, shall have the meanings specified below:

- a. **Digital Watermarks.** Visibly imperceptible or barely visible information embedded into a digital image that can be interpreted by a Detector.
- b. **Special Watermarks.** Digital watermarks that will have distinguishing characteristics for the purpose of providing added counterfeit deterrence for currency notes.
- c. **Common Marks.** Pre-existing indicators that can be used to identify currency notes, including Small Circles for SSG-2 countries, Small Circles for non-SSG-2 countries, the U.S. Treasury seal, the SSG-2 Experimental Seal, and the Bank of Japan seal.
- d. **Embedder.** A computer program that can embed a Special Watermark into a currency note design.
- e. **Detector.** A computer program that accepts a bit-map representation of an image and determines if the image represented by the bitmap contains a Special Watermark.
- f. **Intellectual Property.** Includes but is not limited to patents, copyrights, trademarks, and trade secrets.

2. **Research and Development by Digimarc**

a. **Demonstration.** Digimarc will demonstrate watermark detection using currency notes at the SSG-2 Plenary Meeting on June 12, 1998, or at such other time and place as Digimarc and SSG-2 shall specify in writing signed by authorized representatives of each of them.

1) Prior to the demonstration specified in Paragraph 2.a. above, SSG-2 will provide Digimarc with:

A) Two (2) experimental single-sided currency notes to watermark, consisting of one (1) computer generated design (Dutch Experimental Design); and one (1) generated from scanned film origination (Millais Design), which two (2) experimental currency notes Digimarc will watermark at a single watermark durability level for printing at 1000 dpi and will return to SSG-2 Digimarc prior to the demonstration specified in Paragraph 2.a. above; and

B) Two (2) proofed wet and dry offset experimental currency notes for use in testing watermark detection.

b. **Final Report.** On or before December 31, 1998, Digimarc will prepare and deliver to SSG-2 a written final report which shall contain, among other things, an analysis of test results; a discussion of opportunities to improve the technology; an analysis of intaglio and letterpress feasibility; an analysis of aesthetics vs. robustness; and an analysis of the feasibility of integrating recognition of existing deterrent features (notably Common Marks) into the detection system.

3. **Intellectual Property**

a. **SSG-2 Intellectual Property.** All intellectual property provided by SSG-2 hereunder will be the sole property of SSG-2.

b. **Digimarc Intellectual Property.** All intellectual property provided by Digimarc hereunder will be the sole property of Digimarc.

4. **SSG-2 Liability**

a. Within twenty (20) days after the date of execution of this Agreement, SSG-2 will pay Digimarc the amount of five hundred thousand U.S. dollars (\$500,000.00).

b. Digimarc expressly acknowledges that this Agreement is entered into by SSG-2 as an organization only, and that no liability is created or shall arise hereunder on the part of any individual member or members of SSG-2, or the representatives, officers, agents, or principals of any of them; and Digimarc hereby expressly waives any such claims as may now exist or arise in the future.

c. Digimarc expressly acknowledges that SSG-2's sole obligation to Digimarc hereunder is the payment provided for in Paragraph 4.a. above, and that no other liability or obligation now exists or shall arise under this Agreement to Digimarc, or to any of Digimarc's representatives, officers, employees, agents, principals or assigns, under any legal or equitable theory or otherwise; and Digimarc hereby expressly waives any such claims as may now exist or arise in the future.

5. **Governing Law and Jurisdiction**

a. **Governing Law.** The interpretation of this Agreement, and all disputes concerning this Agreement or concerning the performance of the parties hereunder, shall be governed by the laws of the United States of America and, to the extent not inconsistent therewith, the laws of the District of Columbia.

b. **Jurisdiction.** The parties to this Agreement expressly consent to the jurisdiction of the federal and District of Columbia courts located in the District of Columbia with respect to disputes concerning the interpretation of this Agreement or the performance of the parties hereunder.

05/00 80 10.20 +41 01 225 7000 BIS - HK1 - B12
00041 01 400 2100 D.1.3. BASEL 05.00.1990 10.00 F.010(010)
01010

6. **Notices**

All notices concerning this Agreement shall be delivered as follows:

a. If to Digimarc:

[REDACTED] President and CEO
Digimarc Corporation
1 Center Pointe Drive, Suite 500
Lake Oswego, OR 97035

b. If to SSG-2:

[REDACTED]
Monetary and Economic Department
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

with copies to:

[REDACTED]
Assistant to the Board
Board of Governors of the Federal Reserve System
Washington, DC 20551

and

[REDACTED]
Chief Scientist
Bank of England Printing Works
Langston Road
Loughton
Essex, IG10 3TN
U.K.

7. **Validity and Severability**

The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.

8. **Entire Understanding, Modification**

a. This Agreement constitutes the entire understanding of the parties regarding the subject matter hereof and supersedes any prior verbal or written Agreements or representations by either Digimarc or SSG-2 concerning the subject matter hereof; provided, however, that this Agreement shall not supersede or modify any of the obligations of confidentiality in the previously executed Non-Disclosure Agreement between Digimarc and SSG-2.

b. This Agreement cannot be modified except in writing and signed by a duly authorized representative of Digimarc and by a duly authorized representative of SSG-2.

Agreed to and effective as of the date first hereinabove written.

Digimarc Corporation

By:

Signature: _____

Title: President and CEO

SSG-2

By:

Signature: _____

Title: Chairman of SSG-2

By:

Signature: _____

Title: Immediate Past Chairman of SSG-2

33162_1.DOC

Appendix C

**PROPOSED FINANCIAL REQUIREMENT FOR SSG-2 WORKING PARTY
1/6/98 - 31/5/2000**

For details of Work Programme see Appendix A.

1 PERIOD 1/6/98 - 31/5/1999 (YEAR 1)

1.1 Travel

Possible 7 meetings in the USA:	£150,000
Possible 2 meetings in Japan:	£ 25,000
Possible 4 meetings in Europe:	£ 35,000
Total:	£210,000

1.2 Test Programme not included in Account Statement Appendix B

Printing:	£30,000
Adversarial Analysis:	£10,000
Total:	£40,000

TOTAL FOR YEAR 1: £250,000

2 PERIOD 1/6/99 - 31/5/2000

Possible 4 meetings in USA:	£ 80,000
Possible 3 meetings in Europe:	£ 20,000
Total:	£100,000

TOTAL FOR YEAR 2: £100,000

3. TOTAL REQUIREMENT FOR YEAR 1 + YEAR 2 = £350,000

4. MONEY AVAILABLE

From Appendix B, balance available:	£164,800
Interest accrued (estimate):	£ 11,000
TOTAL AVAILABLE (ESTIMATE):	£175,800

5. RECOMMENDATION

It is recommended that a subscription is levied for year 1998/1999 in December 1998. This would raise (at current rates) £266,800 and should be sufficient to cover the year 2 (1999/2000) unless the Work Programme changes. It is suggested that the Steering Committee are empowered to raise a further subscription if this is seen to be necessary.

Appendix D

SSG-2 Plenary Meeting, Stockholm 12 June 1998

Proposals for Future Funding of SSG-2

The Steering Committee have suggested that in future the SSG-2 should be funded on the basis of GDP rather than the current system based on circulation value in US dollars.

A proposed scheme is attached in which rounded values of GDP form the basis for the share of expenses paid by each country. Also shown is the effect of the formation of the Euro grouping into an ECB.

The implications of such a change will be debated at the meeting.

TABLE 1

Confidential

1

Appendix D

Funding of SSG2 (Proposed)

	GDP(1997)		Band		Level		A
	\$bn		Power of 10		Scale Note A	Units	% Share
OECD	22208.8	22209		22209			
G7	18576.6	18576		18576			
OECD Europe	8702.2	8703		8703			
EU15 (note B)	8093.4	8094	4	0.8094	0.8	8000	
EU11(note B)	6303.4	6304	4	0.6304	0.6	6000	
USA	7819.3	7820	4	0.782	0.8	8000	38.35
Japan	4223.4	4224	4	0.4224	0.4	4000	19.18
Germany	2115.4	2116	4	0.2116	0.2	2000	9.59
France	1393.8	1394	4	0.1394	0.1	1000	4.79
UK	1278.4	1279	4	0.1279	0.1	1000	4.79
Italy	1146.2	1147	4	0.1147	0.1	1000	4.79
Canada	599	599	3	0.599	0.6	600	2.88
Spain	533.4	534	3	0.534	0.5	500	2.40
Australia	394.7	395	3	0.395	0.4	400	1.92
Netherlands	362.9	363	3	0.363	0.4	400	1.92
Switzerland	252.1	253	3	0.253	0.3	300	1.44
Belgium	242.5	243	3	0.243	0.2	200	0.96
Sweden	229.5	230	3	0.23	0.2	200	0.96
Austria	206.2	207	3	0.207	0.2	200	0.96
Turkey	193.8	194	3	0.194	0.2	200	0.96
Denmark	163	163	3	0.163	0.2	200	0.96
Norway	155.4	156	3	0.156	0.2	200	0.96
Greece	119.1	120	3	0.12	0.1	100	0.48
Finland	117.5	118	3	0.118	0.1	100	0.48
Portugal	97.5	98	2	0.98	1	100	0.48
Ireland	72.7	73	2	0.73	0.7	70	0.34
Czech Rep.	53.4	54	2	0.54	0.5	50	0.24
Hungary	44	44	2	0.44	0.4	40	0.19
						20860	100.00
Luxembourg	16.5	16	2	0.16	0.2	20	
Korea	467.9	468	3	0.468	0.5	500	
Mexico	404.2	405	3	0.405	0.4	400	
Iceland	7.4	8	1	0.8	0.8	8	
New Zealand	66	66	2	0.66	0.7	70	
Poland	136.6	137	3	0.137	0.1	100	

TABLE 1

Confidential

Appendix D

Funding of SSG2 (Proposed)

Additional Information

	GDP(1997)	B	C	D	E	F	G
	\$bn	Euro11	%Share	Euro15	%share	Current Scheme	%
OECD	22208.8						
C7	18575.6						
OECD Europe	8702.2						
EU15 (note B)	8088.4			8000	36.71%		
EU11(note B)	6303.4	6000	28.18		0.00%	4	8.70
USA	7819.3	8000	37.58	8000	36.71%	4	8.70
Japan	4223.4	4000	18.79	4000	18.36%	4	8.70
Germany	2115.4		0.00		0.00%	4	8.70
France	1393.8		0.00		0.00%	3	6.52
UK	1278.4	1000	4.70		0.00%	3	6.52
Italy	1146.2		0.00		0.00%	3	6.52
Canada	599	600	2.82	600	2.75%	2	4.35
Spain	533.4		0.00		0.00%	3	6.52
Australia	394.7	400	1.88	400	1.84%	2	4.35
Netherlands	362.9		0.00		0.00%	2	4.35
Switzerland	252.1	300	1.41	300	1.38%	2	4.35
Belgium	242.5		0.00		0.00%	2	4.35
Sweden	228.5	200	0.94		0.00%	1	2.17
Austria	206.2		0.00		0.00%	2	4.35
Turkey	193.8	200	0.94	200	0.92%	1	2.17
Denmark	163	200	0.94		0.00%	1	2.17
Norway	155.4	200	0.94	200	0.92%	1	2.17
Greece	119.1	100	0.47		0.00%	1	2.17
Finland	117.5		0.00		0.00%	1	2.17
Portugal	97.5		0.00		0.00%	1	2.17
Ireland	72.7		0.00		0.00%	1	2.17
Czech Rep.	53.4	50	0.23	50	0.23%	1	2.17
Hungary	44	40	0.19	40	0.18%	1	2.17
		21290	100.00	21790	100.00%	40	100.00

Note A Scale Values
Rounded to nearest 0.1

Note B Combined EU11 Values 5590.00
Combined EU15 Values 7090.00

Distribution list of the Tracing System (upgraded software) (Completed payment distribution)

COUNTRY	DATE	VERSION ID	ORGANIZATION	TITLE	DEPARTMENT	NAME	ADDRESS	FAX	TEL
Morocco	98/05/06	4.11-1	4001 Gendarmerie Royal	Director	Laboratoire de Recherches et D'Analyses Techniques et Scientifiques	[REDACTED]	B.P.6597 Rabat Institut CP10101 Morocco	[REDACTED]	[REDACTED]
Latvija	98/05/08	4.11-1	4002 Bank of Latvia	Electronic Engineer	Cashier's and Money Operations Department	[REDACTED]	Riga, LV-1050 ,K.Valdemara Iela street 2a	[REDACTED]	[REDACTED]
Republic of Korea	98/06/02	4.11-1	4003 Korea Natonal Police Agency	The Chief of Criminal Identification Sector	Criminal Affair Bureau	[REDACTED]	209 Mikeun-Dong, Seodaemun-ku, Seoul, Korea	[REDACTED]	[REDACTED]
Denmark	98/06/09	4.11-1	4004 Danmarks Nationalbank	Deputy Director	Banknote Printing Works	[REDACTED]	Havnegade 5, DK-1093 Copenhagen	[REDACTED]	[REDACTED]
Austria	98/07/03	4.11-1	4005 OESTERREICHISCHE NATIONALBANK	Ing.	Druckerei fur Wertpapiere	[REDACTED]	Garnisongasse 15 1090 Wien, Austria	[REDACTED]	[REDACTED]
Mexico	98/07/03	4.11-1	4006 Banco de Mexico	Security Manager	Security Department	[REDACTED]	PRESA DE LA AMISTA # 707, MOD. VII, COL. IRRIGACION, C.P. 11500 MEXICO, D.F.	[REDACTED]	[REDACTED]
Switzerland	98/07/03	4.11-1	4007 Banque Nationale Suisse		Cash Department	[REDACTED]	Bundesplatz 1, CH-3003 Berne	[REDACTED]	[REDACTED]
Federal Republic of Germany	98/07/31	4.11-1	4008 Deutsche Bundesbank		Cashiers Department	[REDACTED]	Deutsche Bundesbank, P.O.B. 10 06 02 D 60006 Frankfurt/Main	[REDACTED]	[REDACTED]
Republic of Cyprus	98/08/10	4.11-1	4009 Central Bank of Cyprus	Manager	Domestic Banking Operations Department	[REDACTED]	Central Bank of Cyprus, 80 Kennedy Avenue, P.O BOX 5529 Nicosia, Cyprus	[REDACTED]	[REDACTED]
Australia	98/09/21	4.11-1	4010 Reserve Bank of Australia		Note Printing Australia	[REDACTED]	Hume Highway, Craigieburn, Victoria3064. Australia	[REDACTED]	[REDACTED]
Norway	98/09/30	4.11-1	4011 National Criminal Investigation Service	Head of Document and Handwriting	Laboratory Division- Document And Handwriting Subdivision	[REDACTED]	Fredrik Selmers vei4,0663 Oslo,NORWAY		

Bitmap Tracing System Upgrade

- SA - Form faxed to USSS.
- pan - No need to send - BOJ has forms.
- rmany - Fax to [REDACTED]
- s - Gave to [REDACTED]
- hevlans - Gave to [REDACTED]
- lgium - Gave to Paul
- nada - Gave to Bill
- itzerland - Faxed to Martin
- once - Fax to [REDACTED]
- aly - Fax to [REDACTED]
- emart - Fax to [REDACTED]
- eden - Fax to [REDACTED]
- zin - Fax to [REDACTED]
- ece - Fax to [REDACTED]
- key - Fax to [REDACTED]
- ngary - Fax to [REDACTED]
- stria - Fax to [REDACTED]
- rway - Fax to [REDACTED]
- land - Fax to [REDACTED] - check fax #
- tralia - Fax to [REDACTED] - check fax #
- land - Fax to [REDACTED]
- ec Republic - Fax to [REDACTED]
- rtugal - Fax to [REDACTED]

95 JUL 31 AM 10:32

LE DIRECTEUR GÉNÉRAL
DE LA FABRICATION DES BILLETS

Puteaux, 21 July 1995
RECEIVED
OFFICE OF THE CHAIRMAN

Mr Alan GREENSPAN
Governor
BOARD OF GOVERNORS
OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551
U.S.A.

Dear Mr Governor,

I am writing to you in my capacity as Chairman of the Steering Committee of the Special Study Group 2 (SSG-2) in order to brief you on the progress of the Study Group's work over the last two and a half years. The Study Group was formed in January 1993 by the G-10 central banks in conjunction with the members of European Bank Note Printers Conference and Australia, with a mandate to explore ways of reducing the risk of counterfeiting of banknotes using colour copiers and scanners linked to personal computers.

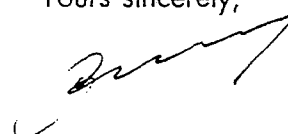
As is explained in greater detail in the attached Executive Summary, the Study Group's work has progressed quite rapidly. Two different technologies are currently available. Should the copier manufacturers agree to install them, these two technologies will enable colour copiers to recognise banknotes and thus to disengage the copying mechanism. It can be expected that it will be possible to equip new copiers with these systems starting in about one year's time but progress has so far been hampered by the resistance of the representation of the Japanese colour copier manufacturers (JBMA) to include the second technology. The Steering Committee is currently trying to convince the JBMA that two different technologies are necessary.

In addition to these two systems, a third system has been developed which enables law enforcement agencies to trace the specific copier used to counterfeit banknotes. This system is already operational.

In connection with copiers, the SSG-2 is expanding its work programme to include scanners linked to personal computers, which constitute a potentially greater counterfeiting threat than copiers. I hope to be able to inform you of the Study Group's progress in this regard in about a year's time.

I am, dear Mr Governor,

Yours sincerely,



A. ARMAND

Chairman of the Steering Committee of the SSG-2

Executive Summary of SSG-2 Activities
January 1993 - June 1995

The *Special Study Group 2* (SSG-2) was established in January 1993 by the G-10 central banks in conjunction with the members of the European Bank Note Printers Conference, who had previously set up a Working Group of technical experts (SSG-1) in order to study the general problem of counterfeiting by means of colour copiers. A *Steering Committee* was also formed to supervise of the SSG-2's work programme and budget. At the suggestion of the Bank of Japan, the Japanese copier manufacturers were encouraged to work with the SSG-2 to develop systems by which colour copiers could recognise banknotes and thereby refuse to make copies.

I. Overview of work to date

The SSG-2 has assessed a large number of alternative technologies for the prevention of counterfeiting using colour copiers, and believes that a combination of two technologies, described below, would provide an effective safeguard against "casual" counterfeiting.

(a) *Common marks*

The first system involves a *common mark*, which is printed on the banknote and is recognised by the colour copier. The mark can either be hidden in the background of the banknote design, or can take the form of an easily recognisable "seal" on the note. Drawbacks of this system are that it will require a redesign of the note and that it may be possible to circumvent if the function of the mark becomes publicly known. The SSG-2 expects that it will be possible to install this system in new copiers as from August 1996. The system has been developed voluntarily by the Omron Corporation of Japan for the Japan Business Machine Makers Association (JBMA), whose members currently account for the whole of the worldwide production of colour copiers.

(b) *Microwave system*

The second system involves printing banknotes on paper incorporating non-magnetic fibres, which can be detected by the copier using *microwave technology*. This system is potentially superior to the common mark system in that it can be introduced into banknotes simply by adding special fibres to the paper and may therefore be technically more difficult to defeat. However, the JBMA is not enthusiastic about also adopting this system because it has no experience in using microwave technology in copiers, and is concerned that compatibility problems may arise.

There is some uncertainty as to when the microwave system will be operational: the SSG-2 believes that the system could be incorporated in copiers as early as next summer, while the JBMA is concerned that it could take as much as 2-3 years to evaluate the system fully. Since some further development work is necessary (e.g. to ensure that paper containing the fibres is fully compatible with all aspects of banknote production and use), the likelihood of a delay is greater with the microwave system than with the common mark system.

The technologies used in the microwave system have been developed by NV Bekaert SA, which holds patents on the manufacture of the fibres and their use for recognition purposes, and Arjo-Wiggins SA, which holds patents on methods of

incorporating the fibres in paper. Licensing and royalty agreements have yet to be reached with these firms.

While there is some uncertainty about the availability of the microwave system, the SSG-2 believes that it is essential that both systems be used jointly. Since the two technologies differ substantially, it would be difficult for counterfeiters to defeat the systems through trial-and-error experimentation. Furthermore, since some central banks may choose to use only one system, the inclusion of two detectors in the copiers would provide central banks with useful flexibility. Finally, the use of both technologies would make it more likely that a solution to the counterfeiting threat posed by scanners linked to personal computers, which constitute a potentially greater threat than colour copiers, could be found without the need to introduce yet another technology. However, the use of both systems in combination, as recommended by the SSG-2, would add to the cost of colour copiers with obvious implications for competitiveness.

(c) *Tracing system*

It should be noted that in addition to these two systems, the JBMA has voluntarily developed a *tracing system* which enables law enforcement agencies to determine the specific machine used to counterfeit banknotes. This system is already operational, and considerably increases the likelihood that counterfeiters of banknotes will be apprehended.

II. Future work

(a) *SSG-2*

In the year ahead the SSG-2 will monitor the final development and implementation of the two anti-counterfeiting systems, and ensure that any technical difficulties are resolved. Given the progress made with regard to copiers, the SSG-2 has been instructed by the Steering Committee to examine, through bilateral contacts with a small number of manufacturers, whether the technologies developed for copiers could also be used for scanner and computer systems. Since medium-sized and small scanners appear to constitute the greatest threat, the SSG-2 will focus its efforts on this segment of the industry.

(b) *Steering Committee*

In order to emphasise the importance attached by the central banks to having both anti-counterfeiting systems incorporated in copiers, the Steering Committee has decided to send a small group of Heads of Delegation to Japan to resolve with the JBMA any difficulties to which this could give rise.

The Steering Committee believes that at some future date legislation may be required to limit the risk of counterfeiting of banknotes using copiers and scanners, in particular by preventing the importation of colour copiers and scanners not equipped with adequate anti-counterfeiting systems. The Committee has therefore decided to set up a small group of experts to explore legal issues that would arise in this context.



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

THEODORE E. ALLISON
ASSISTANT TO THE BOARD
FOR FEDERAL RESERVE
SYSTEM AFFAIRS

Telephone 202-452-2793
Facsimile 202-452-5216

FAX COVER SHEET

To: Ms. Bradbury, Messrs. McNamara and Flynn Date: July 21, 1995
From: Theodore E. Allison

Message or Special Instructions:

Attached is a revised version of the cover letter of the Executive Summary faxed to you yesterday. Please disregard the cover letter faxed to you yesterday.

We _____ are sending the original document by mail.
 x are not.

Number of pages _____

BANQUE DE FRANCE

LE DIRECTEUR GÉNÉRAL
DE LA FABRICATION DES BILLETS

Puteaux, 21 July 1995

Mr Alan GREENSPAN
Governor

BOARD OF GOVERNORS
OF THE FEDERAL RESERVE SYSTEM

WASHINGTON, D.C. 20551
U.S.A.

Dear Mr Governor,

I am writing to you in my capacity as Chairman of the Steering Committee of the Special Study Group 2 (SSG-2) in order to brief you on the progress of the Study Group's work over the last two and a half years. The Study Group was formed in January 1993 by the G-10 central banks in conjunction with the members of European Bank Note Printers Conference and Australia, with a mandate to explore ways of reducing the risk of counterfeiting of banknotes using colour copiers and scanners linked to personal computers.

As is explained in greater detail in the attached Executive Summary, the Study Group's work has progressed quite rapidly. Two different technologies are currently available. Should the copier manufacturers agree to install them, these two technologies will enable colour copiers to recognise banknotes and thus to disengage the copying mechanism. It can be expected that it will be possible to equip new copiers with these systems starting in about one year's time but progress has so far been hampered by the resistance of the representation of the Japanese colour copier manufacturers (JBMA) to include the second technology. The Steering Committee is currently trying to convince the JBMA that two different technologies are necessary.

In addition to these two systems, a third system has been developed which enables law enforcement agencies to trace the specific copier used to counterfeit banknotes. This system is already operational.

In connection with copiers, the SSG-2 is expanding its work programme to include scanners linked to personal computers, which constitute a potentially greater counterfeiting threat than copiers. I hope to be able to inform you of the Study Group's progress in this regard in about a year's time.

I am, dear Mr Governor,

Yours sincerely,

**Executive Summary of SSG-2 Activities
January 1993 - June 1995**

The *Special Study Group 2* (SSG-2) was established in January 1993 by the G-10 central banks in conjunction with the members of the European Bank Note Printers Conference, who had previously set up a Working Group of technical experts (SSG-1) in order to study the general problem of counterfeiting by means of colour copiers. A *Steering Committee* was also formed to supervise of the SSG-2's work programme and budget. At the suggestion of the Bank of Japan, the Japanese copier manufacturers were encouraged to work with the SSG-2 to develop systems by which colour copiers could recognise banknotes and thereby refuse to make copies.

1. Overview of work to date

The SSG-2 has assessed a large number of alternative technologies for the prevention of counterfeiting using colour copiers, and believes that a combination of two technologies, described below, would provide an effective safeguard against "casual" counterfeiting.

(a) Common marks

The first system involves a *common mark*, which is printed on the banknote and is recognised by the colour copier. The mark can either be hidden in the background of the banknote design, or can take the form of an easily recognisable "seal" on the note. Drawbacks of this system are that it will require a redesign of the note and that it may be possible to circumvent if the function of the mark becomes publicly known. The SSG-2 expects that it will be possible to install this system in new copiers as from August 1996. The system has been developed voluntarily by the Omron Corporation of Japan for the Japan Business Machine Makers Association (JBMA), whose members currently account for the whole of the worldwide production of colour copiers.

(b) Microwave system

The second system involves printing banknotes on paper incorporating non-magnetic fibres, which can be detected by the copier using *microwave technology*. This system is potentially superior to the common mark system in that it can be introduced into banknotes simply by adding special fibres to the paper and may therefore be technically more difficult to defeat. However, the JBMA is not enthusiastic about also adopting this system because it has no experience in using microwave technology in copiers, and is concerned that compatibility problems may arise.

There is some uncertainty as to when the microwave system will be operational: the SSG-2 believes that the system could be incorporated in copiers as early as next summer, while the JBMA is concerned that it could take as much as 2-3 years to evaluate the system fully. Since some further development work is necessary (e.g. to ensure that paper containing the fibres is fully compatible with all aspects of banknote production and use), the likelihood of a delay is greater with the microwave system than with the common mark system.

The technologies used in the microwave system have been developed by NV Bokaert SA, which holds patents on the manufacture of the fibres and their use for recognition purposes, and Arjo-Wiggins SA, which holds patents on methods of

incorporating the fibres in paper. Licensing and royalty agreements have yet to be reached with these firms.

While there is some uncertainty about the availability of the microwave system, the SSG-2 believes that it is essential that both systems be used jointly. Since the two technologies differ substantially, it would be difficult for counterfeiters to defeat the systems through trial-and-error experimentation. Furthermore, since some central banks may choose to use only one system, the inclusion of two detectors in the copiers would provide central banks with useful flexibility. Finally, the use of both technologies would make it more likely that a solution to the counterfeiting threat posed by scanners linked to personal computers, which constitute a potentially greater threat than colour copiers, could be found without the need to introduce yet another technology. However, the use of both systems in combination, as recommended by the SSG-2, would add to the cost of colour copiers with obvious implications for competitiveness.

(c) Tracing system

It should be noted that in addition to these two systems, the JBMA has voluntarily developed a *tracing system* which enables law enforcement agencies to determine the specific machine used to counterfeit banknotes. This system is already operational, and considerably increases the likelihood that counterfeiters of banknotes will be apprehended.

II. Future work

(a) SSG-2

In the year ahead the SSG-2 will monitor the final development and implementation of the two anti-counterfeiting systems, and ensure that any technical difficulties are resolved. Given the progress made with regard to copiers, the SSG-2 has been instructed by the Steering Committee to examine, through bilateral contacts with a small number of manufacturers, whether the technologies developed for copiers could also be used for scanner and computer systems. Since medium-sized and small scanners appear to constitute the greatest threat, the SSG-2 will focus its efforts on this segment of the industry.

(b) Steering Committee

In order to emphasize the importance attached by the central banks to having both anti-counterfeiting systems incorporated in copiers, the Steering Committee has decided to send a small group of Heads of Delegation to Japan to resolve with the JBMA any difficulties to which this could give rise.

The Steering Committee believes that at some future date legislation may be required to limit the risk of counterfeiting of banknotes using copiers and scanners, in particular by preventing the importation of colour copiers and scanners not equipped with adequate anti-counterfeiting systems. The Committee has therefore decided to set up a small group of experts to explore legal issues that would arise in this context.



DEPARTMENT OF THE TREASURY
BUREAU OF ENGRAVING AND PRINTING

WASHINGTON, D. C. 20228

August 22, 1995

MEMORANDUM TO: MEMBERS OF THE ACD STEERING COMMITTEE

FROM: *gaf* THOMAS A. FERGUSON
ASSISTANT DIRECTOR
RESEARCH AND DEVELOPMENT

SUBJECT: ACD STEERING COMMITTEE MEETING
July 11, 1995

Attached are the FINAL minutes from the July 11, 1995 meeting of the Advanced Counterfeit Deterrence Steering Committee.

The next meeting will be held on July 31, at 11:00 am at the Department of the Treasury.

Thank you for your attention.

DEPARTMENT OF THE TREASURY

BUREAU OF ENGRAVING AND PRINTING

WASHINGTON, D.C. 20228

ADVANCED COUNTERFEIT DETERRENCE

STEERING COMMITTEE

FINAL MINUTES

July 11, 1995

The Advanced Counterfeit Deterrence Steering Committee met on July 11, 1995 at the Federal Reserve Board to review the status of the various efforts to enhance the security of United States currency. In attendance were:

Mary Ellen Withrow, Treasurer of the United States

Darcy Bradbury

Sean Flynn

Thomas A. Ferguson - Bureau of Engraving and Printing (BEP)

Robert Stone

Theodore Allison - Federal Reserve System (FRS)

William Stone

Charles Bennett

Edward Coia

Rose Pianalto

James Davidson - U.S. Secret Service (USSS)

James Brown

COUNTERFEIT ACTIVITIES

Mr. Davidson provided an update on USSS activities. The total activity for FY 1995 is \$23 million passed, \$62 million seized, and \$123 million appearing abroad. He noted that of the \$23 million passed in the U.S. 88% were foreign origin with the majority coming from Columbia.

The USSS provided details on the \$50 note first reported on at the June meeting. Analysis of the notes indicates that they have good magnetic qualities but no IMP or taggant. The FRS reported that a total of 16 notes had been found to date and that a system wide sampling would be repeated in 30 days.

FRS DETECTION ACTIVITIES

Mr. Allison reported that the number of counterfeit \$100 notes in foreign deposits was lower than that in domestic deposits for all counterfeit notes. However, the rate of 14342 notes in foreign deposits far exceeded the number in domestic deposits.



Mr. Allison raised the issue of the Federal Reserve Banks not charging back for the circular 20,000 \$50 counterfeit notes. The Steering Committee supported the position that the Bank's not charge back at this time and continue to review the status of this case and monitor the frequency of these notes.

PUBLIC EDUCATION PROGRAM

Ms. Withrow reported that the program is now developing rapidly. Foreign focus groups have been completed and domestic focus groups are scheduled for completion in July. Procurement and budget issues are being reviewed at the Department of the Treasury. She also reported that she met with representatives of Republic Bank during her visit to Tokyo.

Ms. Bradbury reported that she is assembling a dedicated team to handle the information development and rollout. The FRS and USSS are developing programs for their client groups.

Mr. Carter provided a report on the international focus groups. He found the focus groups to be of tremendous value and that a great deal of information was gained. He provided a written report of his observations. The USIA will provide working papers in July and a final report in August. In addition, videos of the sessions are also available.

The ACD Steering Committee was invited to attend any or all of the domestic focus groups. The ACD Steering Committee approved the BEP's creation and release of 6 posters of a new currency type image and 6 blowups of the current \$100 note for use with the domestic focus groups.

Two meetings with the Federal Reserve cash managers and public information officers have been scheduled for late August. The Steering Committee approved the use of overhead depictions of Design B notes for use with these groups. Ms. Bradbury will also provide a briefing for the Conference of First Vice Presidents on July 25 in Philadelphia.

PRODUCTION ISSUES

Mr. Ferguson reported that the BEP would follow the same procedures as 1991 for notifying currency handling equipment manufacturers of the changes and providing notes for them to test. Mr. Allison stated that he would develop a position paper on a user group meeting to get more input from the various segments of cash users. The Steering Committee will review this proposal.

The Steering Committee approved the BEP's release of sheets of printed notes (Design A) to Xerox for verification of the Bureau's taggant control devices. The USSS will be consulted prior to the release of these sheets.

Mr. Coia reported the detectors were on schedule, however, issues with the soil and taggant detectors had been identified. He emphasized that these issues were not "show stoppers."

SSG II

Mr. Allison and Robert Stone reported on the activities of the SSG II. The Group has approved the development of 2 systems, the finger print and the shut down pattern. In the shut down area the SSG II is pursuing the Omron system and the Bekart microwave system. Both the U.S. and Japan are planning on using the Omron system with specific marks reserved for these countries. Other members expressed concern with this plan, although it has always been the U.S.'s stated position.

The SSG II has also proposed that each country review the potential of legislation to require copiers to incorporate the new features. The Treasury's General Counsel will review this issue.

MEETING SCHEDULE

The next meeting of the ACD Steering Committee will be held on July 31, 1995 at 11:00 am at the Bureau of Engraving and Printing.

Bureau of Engraving and Printing

Securities Technology Institute

FAX TRANSMISSION COVER SHEET

14th & C Sts. SW
Washington, DC 20228 USA
Tel: 202-874-3374
Fax: 202-874-3483

Date: 2 June 1998

To: Corinna Balfour

FAX: 9-011-41-61-280-9100

Subject: Agenda/Summary for Plenary Meeting

Sender: Robert G. Stone

You should receive 4 page(s), including this cover sheet.
If you do not receive all pages, please call 202-874-3374.

Dear Corinna:

Please find attached an agenda for the 12 June plenary meeting, and a summary of the past two year's SSG-2 work. I would greatly appreciate it if you could send (fax) these out to all Heads of Delegation, along with the documents provided by Bob Furley and Ted Allison. This should hopefully allow the delegates to prepare for the meeting next week. Thanks for the help.

Sincerely,



1/6/98

AGENDA
Plenary SSG-2 Meeting
Stockholm - 12 June 1998

- 09:00 Opening Remarks/Introductions
Status Report on Computer Systems
Initial Survey & Discussions
Progress with Digimarc
Agreement for α -phase prototype
- 09:30 Digimarc Presentation/Demonstration
- 10:30 Break
- 11:00 Discussion with Digimarc (Questions/Answers)
- 11:30 Discussion on Computer Systems
Reactions from Delegates on Digimarc Presentation
SSG-2 Interface with Other Organizations
Schedule/Actions/Future Decisions
- 12:30 SSG-2 Membership Status
Revised Financial Model/Funding Allocation
1998-1999 Budget and Work Plan
- 13:00 Lunch
- 14:30 Discussion on Financial Model/Budget/Work Plan
- 15:30 Status Financial Account
Status of Common Mark System - Implementation/Licencing
Status of Checking System
Status of Pressroom System
Status of Bekaert/Arjo-Wiggins System
Status of Tracing System
- 16:00 Future Meetings
- Steering Committee - 29 October 1998 at BIS (tentative)
- Steering Committee - 26 January 1999 at BIS (review Digimarc results)
- All sponsors - 16 February 1999 at BIS (decision on Digimarc)
- 16:30 Any Other Business/Depart

SUMMARY OF SSG-2 ACTIVITIES

June 1996 - May 1998

The SSG-2 has been engaged in four initiatives. Banknote recognition by color laser copiers using Common Marks, and banknote recognition by computer systems using Digital Watermarks have been the primary focus of the work.

1. Color Laser Copiers (Common Marks)

After successfully completing the testing of the Common Mark recognition system in copiers, a Memorandum of Understanding with the JBMA was signed to incorporate the detectors in all new production lines of color laser copiers which started production after January 1, 1997. Installation of the detectors is now underway in color laser copiers from all major copier manufacturers. In addition to the Common Mark (SC1) for SSG-2 sponsoring countries, a different Common Mark (SC2) was developed and made available to non-SSG2 countries for "licence fees" paid to the SSG-2 through the B.I.S. A total of 8 non-SSG2 countries have licenced the SC2 Common Mark.

The latest version of the Checking System Software from Omron had some initial difficulties, but these are being addressed and an improved version of the Manual is being sent out to users.

2. Press Room Unit

Omron has also provided a quote for a unit which could be used as a Quality Control Check on the Common Marks in the Press Room. The unit would be a color copier, modified to provide output as to the number and type of marks detected. This would be produced by Omron if there is sufficient demand for it, and assuming 20 units are sold, cost would be 5,000,000 Yen. Although a questionnaire will be circulated shortly to all Heads of Delegation to determine the extent of any interest in a Press Room unit, it would be helpful if Heads of Delegation could provide preliminary information on any interest at the 12 June meeting in Stockholm.

3. Bekaert System

Although the use of steel fibers in paper was initially rejected by the JBMA as being unsuitable for banknote detection by copiers, a new technique has been proposed by Bekaert and Arjo-Wiggins (in conjunction with PA Technology). This new technique involves the use of special low coercivity magnetic steel fibers in paper. The fibers are detected by a simple radio frequency technique. Although the SSG-2 is cooperating with this development, the viability of this technique for copiers remains to be demonstrated

by Bekaert to the SSG-2 and the JBMA.

4. Tracing System

The Tracing System has proved to be a success with a number of Police Forces around the world in solving crimes or convicting counterfeiters. An up-dated version of the BITMAP ANALYSIS software is now available from the JBMA. The JBMA has requested payment of 500,000Yen for this software up-grade to cover a portion of the development costs. The up-grade includes new manuals and listings of copiers models. Copier manufacturers will continue to provide assistance in identifying specific copiers at no additional cost.

5. Computer Systems (Digital Watermarks)

Following a period of research and discussion, the SSG-2 has embarked on a program to develop banknote detection for use in computer systems. The system is based on the ideas behind the Digital Watermarking techniques used in computer graphics to protect the copyright of images. An initial feasibility study was successfully performed for the SSG-2 by Digimarc, a leading U.S. company in the field. They have now been engaged to work with the SSG-2 on development and testing of an Alpha prototype for consideration by the Steering Committee in early 1999. If this effort is successful, it will be necessary to agree with Digimarc and the computer industry upon a strategy for implementation into computer systems. Any agreements may include software, scanner, printer and computer manufacturers.

The SSG-2 anticipates a number of options may be available for response to recognition of a banknote by the computer system. For example, alteration of the digital data file, alteration of any printed output, and display of a warning are three potential responses. The possible responses may have differing legal implications within the sponsoring countries. A questionnaire will be distributed to Heads of Delegation in the near future to identify possible legal issues on the response of computer systems to banknote recognition.

Although extensive testing must be completed, the modified digital watermark (to be called a DR.marc and standing for document recognition mark, but already known colloquially as "Doctor marc") is expected to be designed to have only a very small effect on banknote designs.

6. Another meeting of all sponsoring countries has been scheduled for 16 February 1999. This meeting will be held at the BIS to decide whether the SSG-2 should continue toward implementation of the Digimarc system.

* * * COMMUNICATION RESULT REPORT (JUN. 2.1997 10:57AM) * * *

FILE MODE	OPTION	ADDRESS (GROUP)	TTI BEP-STI	
			RESULT	PAGE
453	MEMORY TX	BALFOUR	OK	P. 4/4

REASON FOR ERROR

E-1) HANG UP OR LINE FAIL
E-3) NO ANSWER

E-2) BUSY
E-4) NO FACSIMILE CONNECTION

Bureau of Engraving and Printing

Securities Technology Institute

FAX TRANSMISSION COVER SHEET

14th & C Sts. SW
Washington, DC 20228 USA
Tel: 202-874-3374
Fax: 202-874-3483

Date: 2 June 1998

To: Corinna Balfour

FAX: 9-011-41-61-280-9100

Subject: Agenda/Summary for Plenary Meeting

Sender: Robert G. Stone

BANK FOR INTERNATIONAL SETTLEMENTS, BASLE/SWITZERLAND

TELEFAX TRANSMITTAL COVER SHEET

Transmission priority: regular

File:
03-31-37

Date: 17th June 98

Number of pages (including cover sheet): 8

To:

Fax No: [REDACTED]
OESTERREICHISCHE NATIONALBANK
For the attention of: [REDACTED]

Fax No: [REDACTED]
BANQUE NATIONALE DE BELGIQUE
For the attention of: [REDACTED] Chef du Département de l'Imprimerie

Fax No: [REDACTED]
BANK OF CANADA
For the attention of: [REDACTED] Department of Banking
Operations

Fax No: [REDACTED]
CZECH NATIONAL BANK, STATE PRINTING WORKS ON SECURITIES
For the attention of: [REDACTED] Technical Manager

Fax No: [REDACTED]
DANMARKS NATIONALBANK
For the attention of: [REDACTED] Director, Banknote Printing Works

Fax No: [REDACTED]
BANQUE DE FRANCE
For the attention of: [REDACTED] Directeur Général de la Fabrication
des Billets

Fax No: [REDACTED]
DEUTSCHE BUNDESBANK
For the attention of: [REDACTED] Vertreter der Hauptabteilung
Hauptkasse

Fax No: [REDACTED]
BANK OF GREECE, BANKNOTE PRINTING WORKS
For the attention of: [REDACTED]

Fax No: [REDACTED]
HUNGARIAN BANKNOTE PRINTING CORPORATION
For the attention of: [REDACTED] General Manager

If this transmission is not complete, please call (41) 61/280 85 85

B.I.S., Basle, Switzerland

Telefax numbers: (41) 61/280 91 00

(41) 61/280 81 00

Telex number: 962487

Telephone number: (41) 61/280 80 80

Transmitted by
(For internal use only)

17.06.1998 11:22

BANK FOR INTERNATIONAL SETTLEMENTS, BASLE/SWITZERLAND

TELEFAX TRANSMITTAL COVER SHEET

To: Fax No: [REDACTED]
CENTRAL BANK OF IRELAND
For the attention of: [REDACTED] Assistant Director General

Fax No: [REDACTED]
BANCA d'ITALIA
For the attention of: [REDACTED] Condirettore Centrale
Capo del Servizio Fabbricazione Carte Valori

Fax No: [REDACTED]
THE BANK OF JAPAN
For the attention of: [REDACTED] Director, Issue Department

Fax No: [REDACTED]
DE NEDERLANDSCHE BANK
For the attention of: [REDACTED], Deputy Director Sector
Payments

Fax No: [REDACTED]
NORGES BANK SEDELTRYKKERI, Oslo
For the attention of: [REDACTED] Director

Fax No: [REDACTED]
BANCO DE PORTUGAL
For the attention of: [REDACTED] Deputy Manager - Currency Issue
Dpt.

Fax No: [REDACTED]
FABRICA NACIONAL DE MONEDA Y TIMBRE, Madrid
For the attention of: [REDACTED] Engineering Manager

Fax No: [REDACTED]
SCHWEIZERISCHE NATIONALBANK
For the attention of: [REDACTED] Direktor, Bereich Bargeld

Fax No: [REDACTED]
CENTRAL BANK OF THE REPUBLIC OF TURKEY
For the attention of: [REDACTED], Vice Governor

Fax No: [REDACTED]
BANK OF ENGLAND
For the attention of: [REDACTED], General Manager
Bank of England Printing Works

If this transmission is not complete, please call (41) 61/280 85 85

B.I.S., Basle, Switzerland

Telefax numbers: (41) 61/280 91 00

(41) 61/280 81 00

Telex number: 962487

Telephone number: (41) 61/280 80 80

Transmitted by
(For internal use only)

BANK FOR INTERNATIONAL SETTLEMENTS, BASLE/SWITZERLAND

TELEFAX TRANSMITTAL COVER SHEET

To: **Fax No:** [REDACTED]
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
For the attention of: [REDACTED]
Assistant to the Board for Federal Reserve System
Affairs, Office of Board Members

Fax No: [REDACTED]
AB TUMBA BRUK
For the attention of: [REDACTED] Director

Fax No: [REDACTED]
BANK OF ENGLAND PRINTING WORKS
For the attention of: [REDACTED], Chief Scientist

Fax No: [REDACTED]
BUREAU OF ENGRAVING AND PRINTING, DEPARTMENT OF THE TREASURY
For the attention of: [REDACTED]

From: [REDACTED]
Secretary SSG-2
Coordinating Services for Central Banks and International Organisations

Ref./Comments:

On behalf of the Chairman, please find attached the draft minutes of the meeting of SSG-2 held on 12th June 1998. I should be grateful for comments by 6th July.

Kind regards,

[REDACTED]

If this transmission is not complete, please call (41) 61/280 85 85

B.I.S., Basle, Switzerland
Telefax numbers: (41) 61/280 91 00
(41) 61/280 81 00
Telex number: 962487
Telephone number: (41) 61/280 80 80

Transmitted by
(For internal use only)

16th June 1998

1
2
3 **Minutes of SSG-2 Plenary Group Meeting**
4 **held in Stockholm, 12th June 1998**
5
6
7

8 M. Armand opened the meeting by thanking Tumba Bruk for hosting it; he went on to welcome
9 Portugal, which had just joined the SSG-2 and then noted that there was no representation from
10 Finland. Finally, he mentioned that he was stepping down from the Chairmanship, partly for the sake
11 of rotation, but also because most of the work was now in the US. In this context, he was delighted
12 that Mr. Allison had been offered the post and had accepted; the changes had been endorsed by the
13 G10 Governors in a recent meeting.
14

15 **1. Report and discussion on computer systems**

16 ***1.1 Presentation***

17 Dr. Furley described briefly the history of the digital watermarking project with Digimarc,
18 noting that agreement had been reached on the programme for the alpha phase, which was scheduled
19 to finish in November 1998.

20 This was followed by a presentation by Digimarc of the document recognition marks, which had
21 been used in other areas and were now being extended to the bank note printing process. Action could
22 be taken to combat copying of bank notes at different stages in the process: the scanning, the opening
23 of the file and the printing. Digimarc would need guidance as to what actions would be appropriate,
24 both from the legal point of view and from the point of view of the process. In other cases (such as
25 vidcos), the aim had been to communicate ownership, so something else would be needed for bank
26 notes. It seemed that it might also be possible to include detection of the common marks, some work
27 having already been done with the scal type mark. It was noted that the digital recognition marks
28 provided other opportunities, such as interfering with a search on the Internet.

29 A number of questions were raised about the technique and its application to the bank note
30 printing process. These included possible problems with intaglio printing, as opposed to offset (where
31 there might be difficulties in incorporating the marks into an existing design), the effect on the speed
32 of the scanning and copying process (which should be negligible), the penetration of the market
33 (which, in Digimarc's view, depended initially on its deployment by the note printing industry) and
34 the probability of false/positive identification (which was seen as very unlikely, given that digital
35 information was put into the mark). While it was hoped that there could be a wide degree of common
36 decisions, especially on the detector, some country specific options should be possible, such as on the
37 actions to be taken to prevent copying.

38

39

1.2 Discussion within SSG-2

40

41

42

43

44

45

46

It was suggested that if any country needed further information they should contact Messrs Furley or Stone. For the time being, no further action was needed, as the alpha phase has already been agreed and paid for. Following the report on the first phase, which was due in November, a decision on future work would be needed early in 1999. Meetings of the Steering Committee and the Plenary Group in Basle had been planned for January and February respectively. Delegates were also reminded that all the information should be treated as commercially confidential within their own organisation.

47

48

49

50

51

52

53

54

55

56

57

In the tour de table which followed, all participants expressed positive reactions to the first phase, with virtually no reservations. The technique appeared promising for the future, especially with the growing threat of counterfeiting using scanners and personal computers, but clearly more information was needed before any commitments could be made for the second phase. Areas of uncertainty included the robustness of the software against hacking, the speed of market penetration for the software and the final costs, where more information was needed as to the size of the market, so that an open-ended commitment for payment of royalties was avoided. It was unfortunate that the timing of the work meant that the system might not be ready in time for the early production of the euro note, but it was suggested that it should be introduced into the print run as soon as it became available, possibly for the middle denomination notes; suggestions on this would be included in the final report from the SSG-2 Working Group.

58

59

1.3 Other organisations

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

Messrs Stone and Furley mentioned that, although they had initially been comfortable that Digimarc was the only organisation capable of developing the digital recognition system, there were now other companies in this field and they would be grateful for guidance in how to deal with these other companies, in order to avoid subsequent problems. In discussion, it was agreed that it was important to be even-handed; in particular, it had been agreed for the specification of the euro note that there should be no feature with a single source supplier. In theory, the same principle should be followed as for the common mark system, where the marks themselves were the property of SSG-2 and any company coming up with an image recognition product could develop its own. However, in the case of the digital recognition marks, Digimarc had used some of its "own" intellectual property to adapt an existing system for bank notes, so that it would be harder to identify what might be defined as the property of SSG-2. It was agreed that this question of the ownership of the intellectual property should be included in the final signed agreement with Digimarc and a letter would shortly be drafted by Messrs Furley and Stone to open the issue with them; there would also need to be consultations with the lawyers.

75 2. **SSG-2 membership, budget and funding**

76 2.1 **SSG-2 membership**

77 The Chairman welcomed Portugal to the meeting, noting that both Portugal and Luxembourg
78 had been invited to join the SSG-2, at the suggestion of the management of the ESCB. The reason for
79 this was that they would both be issuing euro notes, which will use the common marks, so it was felt
80 that they should have a right to participate in the decision and a duty to support the research
81 financially. A reply was still awaited from Luxembourg, but changes in the management structure
82 were occurring there, which might have delayed an answer.

83

84 2.2 **Funding allocation**

85 Mr. Allison mentioned that the present key to share the funding (using four hands based on
86 figures for notes issued) was satisfactory if only small amounts of funding were required. However,
87 once the amounts became larger, the structure should be re-considered, so that contributions were
88 more closely related to the scale of note issue or counterfeiting. Another question was the move to the
89 ECB once euro notes were issued; the 11 individual central banks could be considered in terms of, say,
90 their individual GDPs, whereas the previous system would have left the ECB as a single central bank.

91 Dr. Furley had circulated tables with a number of variants for the contributions key. After
92 discussion, it was agreed unanimously that funding should be based on GDP figures, rounded to two
93 significant figures, and that similarly there should be weighted voting, using alternative A in the tables
94 attached to these minutes. The new scheme would become effective from 1st January 1999, which
95 meant for the next subscription. It was also emphasised that the principle of "jointness" continued to
96 be important, that all member countries contributed to a project even if they might not benefit directly.
97 The new system was an attempt to find a balance between the traditional system and something which
98 better reflected the level of spending and ability to pay.

99

100 2.3 **Budget and work programme**

101 Dr. Furley presented the budget for the period up to mid-2000, together with the work
102 programme for the first phase of the Digimarc project and some allowance for additional meetings in
103 the following year. This totalled £350,000 and would require a subscription to be paid in early 1999;
104 such a subscription would raise about £266,000 at current rates. No allowance had been made for
105 further payments to Digimarc for subsequent phases of the project and, so that the central banks could
106 include an allocation in their budgets for 1999, it was agreed that the payment of \$1.5 million (around
107 £900,000) should be included as a tentative payment to Digimarc in the first half of 1999 for research
108 in the later stages. Any payment would need final approval from the SSG-2 Plenary Group meeting in
109 February.

110 **3. Other matters**

111 **3.1 Bekaert/Arjo Wiggins system**

112 Dr. Furley reported on the latest state of play with the development of the second system to
113 combat counterfeiting using colour copiers, which was being developed by Bekaert and Arjo Wiggins,
114 now using radio waves. Although this appeared more promising than the steel fibres, it was still
115 necessary for Bekaert and Arjo Wiggins to convince the JBMA of the viability of the system; a
116 meeting would be held in July to this end. The Newsletter would include a report on developments. It
117 was agreed in a tour de table that the system was still worth pursuing.

118

119 **3.2 Tracing system**

120 An updated version of the system was now available and, although the JBMA had hitherto met
121 all the costs, SSG-2 was now being asked to pay ¥500,000 for this initial upgrade, with further
122 upgrades every two years. Delegates were also reminded to let the SSG-2 Working Group know
123 quickly if they encountered problems with getting information from any individual copier
124 manufacturers.

125

126 **3.3 Press room unit**

127 Omron had developed a checking system which could be used in the Press Room, which they
128 were prepared to make available at ¥5 million each, provided 20 units were sold. A questionnaire
129 would be sent out to establish the demand.

130

131 **3.4 Checking system**

132 A new version of the checking system was now available, with a revised manual.

133

134 **4. Future meetings**

135 The Steering Committee would meet in Basle on 26th January 1999, with a meeting of the
136 Plenary Group following on 16th February, also in Basle, to review and take decisions on the second
137 phase of the Digimarc project. A meeting of the Steering Committee had been tentatively scheduled
138 for 29th October 1998 in Basle, but the date would be confirmed if it were felt that the meeting was
139 necessary.

140

141 **5. Any other business**

142 Mr. Holm reported that, following his retirement, Mr. Färber would represent his constituency
143 on the Steering Committee as from 1st February 1999.

144 The ECB had been invited to participate in the BPC as an observer, so it was agreed that they
145 should also participate in the SSG-2 (including the Steering Committee), on the same basis, in the
146 future.

**List of participants in the
SSG-2 Plenary Group Meeting in Stockholm
on Friday, 12th June 1998**

Austria

Belgium

Canada

Czech Republic

Denmark

France

Germany

Greece

Hungary

Ireland

Italy

Japan

Netherlands

Norway

Portugal

Spain

Sweden

Switzerland

Turkey

United Kingdom

United States

SSG-2

BIS



DEPARTMENT OF THE TREASURY
BUREAU OF ENGRAVING AND PRINTING
WASHINGTON, D. C. 20228

September 9, 1997

Mr. Dennis F. Lynch
Special Agent in Charge
Counterfeit Division, Suite 730
United States Secret Service
1800 G Street, NW
Washington, D.C. 20223

Dear Dennis:

At the most recent Special Studies Group (SSG-2) meeting in Tokyo the Japanese Business Machine Maker's Association (JBMA) informed the SSG-2 that an upgrade of the Bitmap tracing system software was being prepared. The upgrade is needed to include new model copiers in the software, as well as to adapt the software for changes in computer systems. The JBMA further indicated that additional upgrades could occur about every 2 - 3 years, as additional copier models are placed on the market and further changes occur in computer systems.

To date, the JBMA has absorbed all costs associated with developing and maintaining the bitmap software. They now wish to charge software users for these costs under a licencing agreement, and proposed the following:

1. The initial upgrade would be licenced to each country for a fee of 500,000 Yen. Each country would be required to designate to the JBMA (Mr. Michio Mogi) an organization and person as a contact point and custodian for control of the software. Copies could be made, as the custodian deems appropriate, for use within the licenced country.
2. Subsequent upgrades would cost 200,000 Yen per country.
3. Upgrades will include new manuals/contact list for copier manufacturers/list of applicable machines.

I have attached the two "Draft" documents provided by the JBMA regarding their proposed plans. The consensus of the SSG-2 Working Party was that the costs proposed by the JBMA appear reasonable, considering the limited usage of the software and the service provided in responding to requests for copier information. The JBMA also agreed that any problems with the bitmap software, including concerns with the response time for providing copier information, should be referred to the JBMA ([REDACTED]).

We were also informed that no changes/improvements have occurred with the Add-on-Dot tracing system.

If you have any questions or concerns with this letter, please call. The address for contacting [REDACTED] is:

[REDACTED]
Secretary CPT-WG
Japan Business Machine Maker's Association
Shuwa Dai-ni Toranomom Building
1-21-19 Toranomom, Minato-ku
Tokyo 105, Japan
Tel: [REDACTED]
Fax: [REDACTED]

Sincerely

[REDACTED]
Program Manager

cc T. Ferguson

28 July 1997

CPT-WG, JBMA

An Action Plan for Providing Decoding Software for Payment

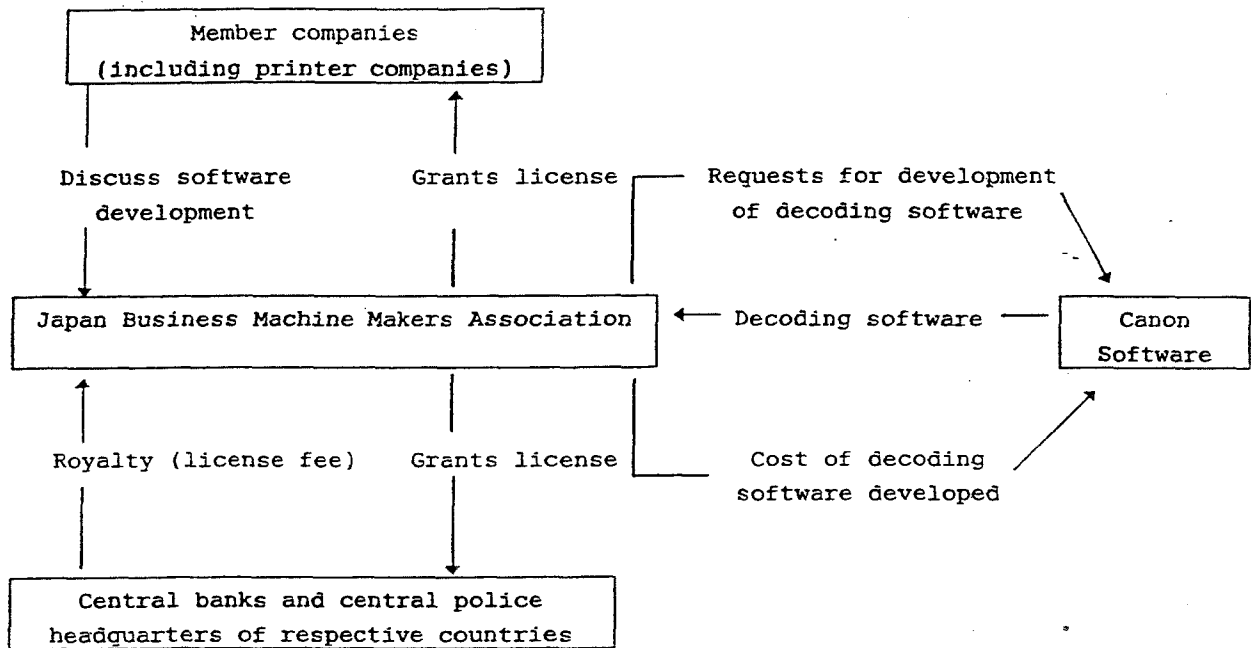
(Draft)

1. Introduction

The counterfeit of bank note which was made easier because of popularization of color copying machines, has now been proved to be effectively prevented by the decoding software recently developed. Future maintenance of the decoding software has reached a critical stage. Indeed, it is a social obligation for all parties involved to see that the decoding software is supplied on a stable basis.

So far, the decoding software has been developed entirely at the expense of the Japan Business Machine Makers Association. With a view to sharing of the future software development and maintenance costs among the beneficiary parties on an equitable basis, we wish to propose that the decoding software in the future be provided for payment under an action plan, as outlined below..

2. Scheme for Providing Decoding Software, for Payment, and for Maintenance Cost



3. Future Upgrade for New Version and Estimated Development Costs of Decoding Software

	Upgrade for New Version for	Estimated development costs
1	Changes in development circumstances	¥7,000,000
2	Adapting to developing operating systems	¥750,000
3	Adapting to developing peripheral equipment	¥750,000
4	New entries of color equipment makers into market	Payable by newly entering makers

* Version ups under 2 through 4 may be expected to take place every 2-3 years.

4. Recovery of Development Costs by Releasing Decoding Software for Payment

Basic approaches to method of recovery:

- Grant a license to each country which uses the decoding software.
- For registration of a user (or for initial license registration), as differentiated from upgrade for new version cases, charge basic fee (for development cost).
- Inquiries from users will be restricted to the central bank/central police headquarters, to hold down cost of the administration of this plan and of maintenance of the support center.
- The support center will be provided with simulation equipment to enable the Association to properly answer inquiries.

5. Maintenance Costs of Decoding Software for 6 Years Simulated:

Prerequisites:

- License to be granted eventually to 30 countries.
- Copying machine makers to pay: ¥500,000/a company
- Initial registration fee for initial year:

¥500,000/a country

- Upgrade fee: ¥200,000/a country

Currency unit: ¥1,000

	1 st yr. 1997	2 nd yr. 1998	3 rd yr. 1999	4 th yr. 2000	5 th yr. 2001	6 th yr. 2002
Income						
User registration fees (No. of countries)		11,000 (22)	4,000 (8)	0	0	0
Upgrade fees (No. of countries)				4,400 (22)	1,600 (8)	4,400 (22)
Total costs to makers	5,000					
Sub-totals	5,000	11,000	4,000	4,400	1,600	4,400
Expenditure						
Administration and support expenses		5,000	4,000	3,000	2,000	2,000
Costs of changes in development environments	7,000					
Cost of upgrade			1,500		1,500	
Expense for equipment		2,000		500		500
Sub-totals	7,000	7,000	5,500	3,500	3,500	2,500
Annual balances	-2,000	4,000	-1,500	900	-1,900	1,900
Aggregate annual balances	-2,000	2,000	500	1,400	-500	1,400

6. Problems to be Studied further:

- Assistance and cooperation must be sought from the central banks of respective countries for providing a center for supplying the decoding software and for controlling redistribution thereof within their own countries.

- In the event the number of licensee countries become more than 30, the upgrade for new version fees to be collected from each licensee countries will be reduced proportionately so there will be no gain as a whole on the part of the Association as a result.

7. Supplemental Information:

(1) For what the "Administration and support expenses (includes those for jobs assigned outside on a contract basis) are?

- Control of the decoding software register.
- Distribution of the decoding software.
- Response to inquiries (user support), e.g., tracing troubles of personal computers.
- Holding and managing seminars.

(2) For what the "Expense for equipment" is?

- Standard type personal computers, scanners and SCSI boards for each of the makers, for verifying operation and tracing.

Attachment 2

28 July 1997

CPT-WG, JBMA

DECODING SOFTWARE DISTRIBUTION AND CONTROL REGULATIONS

(DRAFT)

1. Objective:

The objective of these Regulations is for the CPT-WG, Copying Machine Group, Japan Business Machine Makers Association, hereinafter "CPT-WG," to distribute, on a safe and secure basis, certain decoding software designed to identify, from image data shown on a counterfeited copy made through a color copying machine, the specific color copying machine so used, whereby to support criminal investigations.

2. Application:

These regulations apply to distributions, method of distribution, adoption, amendment and repeal, and records of adoption and amendments, relating to distribution of the decoding software.

3. Distribution:

The decoding software consists of a floppy disk on which the decoding software is recorded, hereinafter "FD," the operating manual thereof and the contact person list showing persons to be contacted.

3.1 FD:

The CPT-WG Secretariat, hereinafter "Secretariat," shall securely keep the master FD obtained from the developer thereof. Secretariat shall reproduce FDs for distribution from the Master FD. The Master FD and reproduced FDs shall be recorded on and controlled by use of the decoding software register.

3.2 Operating Manual:

Secretariat shall securely keep either the operating manual, in a hard copy form or master FD form, as the case may be, received from the developer. Secretariat shall copy or print the operating manual, in a hard copy form or master FD form, for distribution. All operating manuals, whether in a hard copy form, master FDs, or printed form for distribution, shall be registered on and controlled by use of the decoding software register.

3.3 Contact Person List:

Secretariat shall annually obtain from each member company selling color copying machines, a contact person report, from which it shall prepare a contact person list, which shall be copied for distribution purpose. The report and the contact person list for distribution shall be controlled by use of the decoding software register.

4. Distribution:

On request of the central bank or central police headquarters of any country, and before sending out the decoding software, Secretariat shall identify the requesting party, send to and receive from the requesting party a preliminary inquiry/confirmation form, and confirm receipt of the payment for the product to be supplied.

4.1 Identification:

Any inquiry form, which shall be either a facsimile message or letter, from the central bank or central police headquarters of a country shall be referred at least once to the SSG-2 secretary or the embassy in Japan from that country, for identification processes on the part of that country.

4.2 Sending out Preliminary Inquiry Form:

On receipt of a request form from the central bank or central police headquarters of a country, Secretariat shall send out the Preliminary Inquiry form, as per the enclosed specimen, setting forth among other things the name of the person claiming receipt of the decoding software, his address, and organization to which he reports, in addition to the promise form to be completed by him, recommended operating circumstances, and information on payment for the product.

4.3 Confirmation of Receipt of Payment for the Product:

On receipt of the Preliminary Inquiry form, Secretariat shall verify the name and address of the person, claiming receipt of the decoding software, of the requesting party, and confirm that the payment for the product has been received.

4.4 Sending out Decoding Software:

After confirming that the payment for the product has been received, Secretariat shall send out the decoding software and control all decoding software so sent out by way of a register.

5. Adoption, Amendment, Repeal:

These Regulations shall be drafted and, with consent of the CPT-WG, adopted, amended or repealed by the CPT-WG Chairman, with proceedings for adoption and amendments recorded at the end of the text hereof.

6. Records Concerning Adoption and Amendments:

The adopted version (as proposed) was approved by the CPT-WG on _____ (_____), 1997.

_____, 1997

TO:

Japan Business Machine Makers Association

CPT-WG, Copying Machine Group

Secretariat: Michio Mogi

Seiji Okano

Tel: 03-3503-9821

FAX: 03-3591-3646

Preliminary Inquiry (Draft)

Dear sirs,

Thank you for your order for the tracing system.

Kindly complete and return to us this form and make remittance to us in the amount stated below, before we may supply it.

1. Recommended circumstances:

Personal computers: IBM PC/AT compatibles

Memories available: 32 MB or more.

Operating system: Windows 3.1

Scanner: HP 9 (Scan Jet 2 ex); Canon (CJ10); Agfa

(Studio Scan 2 si)

SCSI board: Adaptec (AHA-1542B, AHA-2940)

2. Remittance to be made:

Amount: ¥ _____

To: Fuji Bank, Toranomom Branch

Ordinary account

Account name: Japan Business Machine Maker
Association

Account number:

3. Important:

(1) The copyright to this software is and will continue to be held by the Japan Business Machine Makers Association.

(2) This software is licensed to a country, as represented by the central bank, central police headquarters, or a central government entity, as the case may be. It will be up to the convenience, and be a problem, of that central bank, central police headquarters or central government entity, whether, on its own initiative and responsibility, to sublicense it or not. The Association will not be concerned howsoever with any consequences thereof.

(3) A set, only a set, of the master system will be supplied for a country.

(4) The Company assumes no liability for whatever consequences of use of this software and/or manual therefor.

4. Promise:

(1) I will control, using the control register, any redistribution of this software within the country, which I may arrange, so that it will not be made available for crime purposes.

(2) For confidentiality purposes, no other individuals than I, who am the only authorized agency of the government in this regard, will inquire about details of this software.

Promiser (Custodian):

Country name:

Address:

Tel:

Name of organization:

Name:

FAX:

* * * COMMUNICATION RESULT REPORT (SEP. 9.1997 3:03PM) * * *

FILE MODE	OPTION	ADDRESS (GROUP)	RESULT	PAGE
311	MEMORY TX	94356776	OK	P. 15/15

TTI BEP-STI

REASON FOR ERROR

E-1) HANG UP OR LINE FAIL	E-2) BUSY
E-3) NO ANSWER	E-4) NO FACSIMILE CONNECTION

Bureau of Engraving and Printing
 Securities Technology Institute
 FAX TRANSMISSION COVER SHEET

14th & C Sts. SW
 Washington, DC 20228 USA
 Tel: 202-874-3374
 Fax: 202-874-3483

Date: 9 September 1997
 To: Mr. Dennis Lynch
 FAX: 435-6776
 Subject: Bitmap Software
 Sender: Robert G. Stone

afternoon any comments and suggestions would be appreciated.
Richard

-----Original Message-----

From: Kevin Connor [mailto:kconnor@adobe.com]
Sent: January 7, 2004 10:17 PM
To: [REDACTED]
Cc: [REDACTED]; [REDACTED]
Subject: Cat's out of the bag...
Importance: High

Richard -

Well, it's taken a little longer than I expected, but the online outcry over CDS in Photoshop CS has finally begun. Check out this thread:

<http://www.adobeforums.com/cgi-bin/webx?13@1.hUXSbwPyS90.268675@.2ccf3d27/0>

Clearly, Adobe needs to put a response in this message thread. I took a look at the communication kit you provided previously, but it seems to be primarily designed for handling press inquiries and customer phone calls. There isn't really a single statement to use for an online forum.

Therefore, I'm going to take a stab at a statement myself. Please let me know if this is acceptable ASAP, and I'll get it posted:

Photoshop CS does include a counterfeit deterrence system (CDS) to prevent the illegal duplication of banknotes. This CDS was created by the CBCDG, a consortium of central banks from around the world. We have included CDS in this release at the request of the CBCDG, who have also worked with other hardware and software manufacturers--some of whom have already shipped other products incorporating CDS.

There appear to be several major concerns and objections repeated throughout this message thread, so I'll try to address each one individually:

1. Performance: CDS does not cause any noticeable slowdown in Photoshop performance. Adobe has taken many steps to ensure that our implementation of this technology does not impact your everyday use of the product for non-currency images.
2. Legal use of notes: It is true that the current implementation of CDS will prevent you from scanning in your own banknotes even if your usage intent is entirely within legal boundaries. Regulations for using banknote images vary by country. It is the responsibility of the central bank in each country to provide images that can be used within the legal guidelines of that country. In other words, if you want to legally reproduce images of the new \$20US bills on a Web site or in a marketing brochure, you can contact the U.S. Bureau of Engraving and Printing for legal images that *can* be opened and manipulated in Photoshop CS. (You can visit them at www.moneyfactory.com.) Similar solutions should be available in other

countries. If you find that your central bank is not providing adequate support to permit legal uses of their banknote images, then you should let them know.

3. Adobe's intentions: With both CDS and activation, there have been lots of concerns about what *might* happen or what Adobe *might* be planning for the future. Let me assure you that, although we need to continue to function as a profitable company while also being a good corporate citizen in the countries where we do business, we spend an enormous amount of time worrying about how to provide the best experience for our customers. A lot of thought went into implementing CDS in a way that would largely satisfy government requests without impacting normal usage. Even more thought went into designing an activation approach that would be unobtrusive for legal users of the product under normal circumstances. Even so, both of these are essentially 1.0 implementations of a feature, analagous to the layers palette in Photoshop 3.0. We realize that there may be room for improvements, particularly if there are corner usage cases that weren't taken into account in our current designs. We do want to hear about your concerns, and we definitely want to hear if anything in Photoshop CS has caused any problems for you. But please don't worry about any nefarious plans on Adobe's part. We became a leader in this market by understanding our customers and doing what's right for them, and all of us at Adobe know that we can't remain successful if we ever lose that focus.

One more parting thought: Counterfeit currency is essentially a hot potato. Whoever holds it last, loses. The person who loses isn't necessarily the counterfeiter. There's no government body in place to "reimburse" people who, through no fault of their own, get paid with currency that turns out to be counterfeit. So, lest you think that CDS in Photoshop has no benefits for the customer, keep in mind that, as digital imaging technology becomes more pervasive, who's to say that *you* wouldn't be the one holding the potato?

This turned out a bit more verbose than I intended, but I guess brevity isn't my strong suit! Anyway, let me know if you have any objections to anything I've said here.

Regards,
Kevin

P.S to Drew - I've included you on this e-mail, because this statement includes some remarks about activation as well.

Haley Dawn

From: Eugenie.E.Foster@frb.gov
Sent: Tuesday, January 06, 2004 11:39 AM
To: Haley Dawn
Cc: Michael.Lambert@frb.gov; Ferguson Tom
Subject: language

Dawn:

Here's what we have so far. Shall we discuss?

Genie

In order to address the increasing use of personal computers, digital imaging equipment and software for illicit purposes, the United States is working with a consortium of central banks that has developed a system to deter the use of this technology in the counterfeiting of bank notes. This group is soliciting the support of the digital imaging and computer industry and cooperating with equipment manufacturers and software developers to facilitate the adoption of the system.

All major inkjet printer suppliers have been working voluntarily with the consortium to deter the counterfeiting of currency by inkjet printers and personal computers. The vendors are phasing deterrence measures into their products over time. This long-term program will be effective only when the deterrence measures have become widely deployed. Printer vendors have agreed not to release details on the deterrence technology or their specific plans for its deployment.

Haley Dawn

From: Eugenie.E.Foster@frb.gov
Sent: Wednesday, January 21, 2004 9:04 AM
To: Haley Dawn
Cc: Michael.Lambert@frb.gov; Ferguson Tom
Subject: images

Hi Dawn,

I have been talking to Adobe and CBCDG representatives. Adobe is very concerned about images for its customers. It is looking like the short term answer will be to refer users to the Bureau for high definition images or files. Can you give me the name and number of a contact at the Bureau that Adobe can use for customer service calls where they are willing to make a request for an image?

In the longer term we need to revisit our options. When do you get back?

Thanks,

Genie

Haley Dawn

From: [REDACTED]
Sent: Wednesday, January 14, 2004 11:45 AM
To: [REDACTED]
Cc: [REDACTED]; Haley Dawn; [REDACTED]
Subject: This note is from [REDACTED]

Kevin,

Sorry to respond a little late to your email messages of yesterday. As I indicated earlier, I'm attending an meeting in Europe and your messages only caught up with me this morning (this also accounts for the wrong email address). It appears that there is a bit more media interest following the AP story and I hope it's not causing you too much grief.

Firstly regarding your earlier email - please be assured that we are very comfortable with the positioning on the difficult questions you are receiving regarding work arounds. It is not the intention of the CDS to be a perfect barrier - it is intended to deter the casual or inadvertent copying of banknotes. The focus you placed on deterring youth and educating the public is exactly the right points to be making. Any vulnerabilities in the system are as a result of the trade-offs made to assure that the functionality and user experience is minimally affected. The central banks will not discuss the technical aspects of any implementation but will say if asked (and I was asked by AP but they didn't include it in the story) that Central Banks share the manufacturers' concern for minimising the impact of CDS on the user experience.

Regarding your later email, I'd like to address your concern's regarding the central bank's efforts to make images available to graphics professionals. As you know banknote reproduction legislation varies from country to country and the approaches by various central banks are different. As a result of the earlier conversation we had, a number of central banks have undertaken steps to assure that reproduction policy and the process for obtaining and using images within that policy aligns with the restrictions imposed by CDS.

The Bank of Canada is introducing a new policy this month that provides a means for images and permission for use to be obtained from the Bank. We are preparing a suite of images that can be used by graphic artist professionals which should be available when the policy is introduced.

The ECB has in place a restricted website available to professional (registered) users that provides high resolution banknote images for use by graphics professionals. They are planning to provide unmarked images on that site also.

In Japan the rules and legislation essentially prohibit the use of bank note images. (applicable legislation is fairly broad and reproduction is viewed generally as a

THIS MESSAGE IS FROM [REDACTED] Page 2 of 2

potential offence). If you have specific feedback from Japanese users I would be happy to forward it to the Bank of Japan for their consideration.

The Swiss National Bank will make images available when in fact it becomes an issue in that country.

Following our previous discussion with the FRB and BEP a number of changes were made to the moneyfactory.com website, which I thought had addressed the concerns raised at the time. I've spoken with Genie Foster at the FRB and she would be happy to continue the discussion with you to determine the best approach to meet the needs of your customers and preserve the security of banknotes (I've copied her on this note). I think the best approach, when asked about the availability of images, is still to direct the questioner to the central bank for response. I hope that the above provides you with some confidence that central banks are acting to address the concerns regarding the availability of banknote images. If you feel it is useful, I'd be happy to talk with you directly when I'm back in the office Friday or organize a teleconference with the FRB, BEP and yourself for early next week. Of course, if you feel it would be helpful to have a face to face, I'm sure we could arrange to get the appropriate people out to your office on fairly short notice.

Kind Regards,
Richard

Any e-mail message from the European Central Bank (ECB) is sent in good faith but shall neither be binding nor construed as constituting a commitment by the ECB except where provided for in a written agreement. This e-mail is intended only for the use of the recipient(s) named above. Any unauthorised disclosure, use or dissemination, either in whole or in part, is prohibited. If you have received this e-mail in error, please notify the sender immediately via e-mail and delete this e-mail from your system.

11/3/2008

Adobe Systems Inc. acknowledged it quietly added technology...

CP Wire

Sat 10 Jan 2004

Section: Business

Byline: BY TED BRIDIS

WASHINGTON (AP) _ Adobe Systems Inc. acknowledged it quietly added technology to the world's best-known graphics software at the request of government regulators and international bankers to prevent consumers from making copies of the world's major currencies.

The unusual concession has angered scores of customers.

Adobe, the world's leading vendor for graphics software, said the secretive technology "would have minimal impact on honest customers." It generates a warning message when someone tries to make digital copies of some currencies.

The U.S. Federal Reserve and other organizations that worked on the technology said they could not disclose how it works and would not name which other software companies include it in their products. They cited concerns that counterfeiters would try to defeat it.

"We sort of knew this would come out eventually," Adobe spokesman Russell Brady said Friday. "We can't really talk about the technology itself."

A Microsoft Corp. spokesman, Jim Desler, said the technology was not built into versions of its dominant Windows operating system.

Rival graphics software by Taiwan-based Ulead Systems Inc. also blocks customers from making copies of currency.

Experts said the decision by Adobe represents one of the rare occasions when the U.S. technology industry has agreed to include third-party software code into commercial products at the request of government and finance officials.

Adobe revealed it added the technology after a customer complained in an online support forum about mysterious behaviour by the new \$649 US Photoshop CS software when opening an image of a \$20 US bill.

Kevin Connor, Adobe's product management director, said the company did not disclose the technology at the request of international bankers. He said Adobe may add the detection mechanism to its other products.

"The average consumer is never going to encounter this in their daily use," Connor said. "It just didn't seem like something meaningful to communicate."

Angry customers have flooded Adobe's Internet message boards with complaints about censorship and concerns over future restrictions on other types of images, such as copyrighted or adult material.

"I don't believe this. This shocks me," said Stephen Burns, president of the Photoshop users group in San Diego. "Artists don't like to be limited in what they can do with their tools. Let the U.S. government or whoever is involved deal with this, but don't take the powers of the government and place them into a commercial software package."

Connor said the company's decision to use the technology was "not a step down the road towards Adobe becoming Big Brother."

Adobe said the technology slows its software's performance "just a fraction of a second" and urged customers to report unexpected glitches. It said there may be room for improvement.

The technology was designed recently by the Central Bank Counterfeit Deterrence Group, a consortium of 27 central banks in the United States, Canada, England, Japan, and across the European Union, where there already is a formal proposal to require all software companies to include similar anti-counterfeit technology.

"The industry has been very open to understanding the nature of the problem," said Richard Wall, the Bank of Canada's representative to the counterfeit deterrence group. "We're very happy with the response."

Some policy experts were divided on the technology. Bruce Schneier, an expert on security and privacy, praised the anti-counterfeit technology.

Another security expert, Gene Spafford of Purdue University, said Adobe should have notified its customers prominently. He wondered how closely Adobe was permitted to study the technology's inner-workings to ensure it was stable and performed as advertised.

"If I were the paranoid-conspiracy type, I would speculate that since it's not Adobe's software, what else is it doing?" Spafford said.

Friday, January 09, 2004

To: PRG Members

From: [REDACTED]

Re: Media Enquiry regarding CDS

Reporter: Ted Bridis
Associated Press
Tel.: 202-776-9462

Request: Information on the Counterfeit Deterrence System, the CBCDG, deployment status, technical support for manufacturers, cost and operation of the system.

The Bank of Canada was contacted by the above reporter following enquiries made at the FRB and Secret Service. The reporter had been contacted by an Adobe user who was monitoring regarding counterfeit deterrence on the Adobe Forum website. He had previously talked with Kevin Connor at Adobe who had referenced the CBCDG in his response (note that this is consistent with the communication plan that has been shared with manufacturers).

In responding to the reporter I used the CDS communications Program for Issuing Authorities Q's and A's. I discussed trends in counterfeiting (shift from offset to inkjet) and the growth that has occurred over the last 5-6 years. Questions regarding the specific technology, participating companies, market share of deployed systems, and participating central banks were declined.

Information shared with the reporter on the CBCDG was consistent with that available from the BIS website, and I declined to answer questions regarding the Bank of Canada's specific role within the CBCDG over the last years – although he indicated an awareness that the Bank's role as Chair ended last year.

The reporter raised questions regarding testing and evaluation of the technology provided to companies and the costs of including that technology in their products. I declined to answer the technical questions but indicated that companies recognize their responsibility to deter the use of their product for currency counterfeiting. I also indicated that companies participate voluntarily and are very concerned about the impact of any technology introduced into their products on both performance and user experience.

The reporter was also interested in the ECB consultation process and was aware that the consultation process had ended.

The PRG should be aware that a story may be published in the national media regarding the CBCDG and CDS and that both manufacturers and CBCDG member's should expect and increased level of enquiries over the next week.

Haley Dawn

From: Cameron Jon
Sent: Tuesday, March 09, 2004 1:08 PM
To: Haley Dawn; Borchard Julie; Ferguson Tom
Subject: FW: statement by the Bank for International Settlements on banknote counterfeit deterrence

FYI

-----Original Message-----

From: Daniel.A.Littman@clev.frb.org [mailto:Daniel.A.Littman@clev.frb.org]
Sent: Tuesday, March 09, 2004 1:02 PM
To: Stone Robert; Cameron Jon; Clarke Lenore; Dinunzio Lisa; Linda.Sawma@clev.frb.org;
Lisa.M.Vidacs@clev.frb.org; Mark.Mullinix@sf.frb.org; Michael.Lambert@frb.gov; Peggy.Korte@clev.frb.org;
Richard.P.Joesting@clev.frb.org; [REDACTED]
Subject: statement by the Bank for International Settlements on banknote counterfeit deterrence

Central banks and technology industry join to combat banknote counterfeiting
<http://www.bis.org/cgi-bin/print.cgi>

9 March 2004

In response to the threat of increasing use of personal computers and digital imaging tools in counterfeiting banknotes, the Governors of the G10 central banks authorised in May 2000 the development by a group of central banks of a system to deter PC-based counterfeiting. At their meeting in March 2004, the Governors took note of important progress in this area.

The Central Bank Counterfeit Deterrence Group (CBCDG) has now developed the Counterfeit Deterrence System, consisting of anti-counterfeiting technologies which prevent personal computers and digital imaging tools from capturing or reproducing the image of a protected banknote.

Several leading personal computer hardware and software manufacturers have voluntarily adopted the system in recognition of the harm that counterfeit currency can cause their customers and the general public. The technology does not have the capacity to track the use of a personal computer or digital imaging tool and consumers will not notice any difference in the performance or effectiveness of products equipped with this technology.

Further information is available on the website www.rulesforuse.org, which has links to the regulations of various countries governing the reproduction of banknotes. In countries where the new technology restricts a user's ability to copy images of banknotes, the central bank (or the appropriate authority) will make available banknote images for reproduction in accordance with its requirements. The www.rulesforuse.org website directs users to the procedures and sources of banknote images for countries where they are available.

What is the CBCDG?

The CBCDG's mission is to investigate emerging threats to the security of banknotes and to propose solutions for implementation by issuing authorities. The CBCDG is a working group of 27 central banks and note printing authorities. Its Chairman is Mr Marc Salade, National Bank of Belgium. Ms Lorraine Laviolette, Bank of Canada, serves as the Project Director of CBCDG activities. The CBCDG meets annually at the Bank for International Settlements (BIS) in Basel, where its secretariat is located.

11/3/2008

Haley Dawn

From: Cameron Jon
Sent: Monday, January 12, 2004 9:27 AM
To: Ferguson Tom; Haley Dawn; Borchard Julie
Subject: FW: Adobe & the BEP

FYI - Article about the digital watermark

-----Original Message-----

From: Daniel.A.Littman@clev.frb.org [mailto:Daniel.A.Littman@clev.frb.org]
Sent: Sunday, January 11, 2004 6:09 AM
To: Stone Robert; Cameron Jon; Clarke Lenore; Dinunzio Lisa; Linda.Sawma@clev.frb.org;
Lisa.M.Vidacs@clev.frb.org; Mark.Mullinix@sf.frb.org; Michael.Lambert@frb.gov; Peggy.Korte@clev.frb.org;
Richard.P.Joesting@clev.frb.org; [REDACTED]
Subject: Adobe & the BEP

Adobe Helped Gov't Fight Counterfeiting

1/10 NewsDay Adobe Systems Inc. acknowledged Friday it quietly added technology to the world's best-known graphics software at the request of government regulators and international bankers to prevent consumers from making copies of the world's major currencies.

The unusual concession has angered scores of customers.

Adobe, the world's leading vendor for graphics software, said the secretive technology "would have minimal impact on honest customers." It generates a warning message when someone tries to make digital copies of some currencies.

The U.S. Federal Reserve and other organizations that worked on the technology said they could not disclose how it works and would not name which other software companies include it in their products. They cited concerns that counterfeiters would try to defeat it.

"We sort of knew this would come out eventually," Adobe spokesman Russell Brady said. "We can't really talk about the technology itself."

A Microsoft Corp. spokesman, Jim Desler, said the technology was not built into versions of its dominant Windows operating system.

Rival graphics software by Taiwan-based Ulead Systems Inc. also blocks customers from making copies of currency.

Experts said the decision by Adobe represents one of the rare occasions when the U.S. technology industry has agreed to include third-party software code into commercial products at the request of government and finance officials.

Adobe revealed it added the technology after a customer complained in an online support forum about mysterious behavior by the new \$649 "Photoshop CS" software when opening an image of a U.S. \$20 bill.

Kevin Connor, Adobe's product management director, said the company did not disclose the technology at the request of international bankers. He said Adobe may add the detection mechanism to its other products.

"The average consumer is never going to encounter this in their daily use," Connor said. "It just didn't seem like something meaningful to communicate."

Angry customers have flooded Adobe's Internet message boards with complaints about censorship and concerns over future restrictions on other types of images, such as copyrighted or adult material.

"I don't believe this. This shocks me," said Stephen M. Burns, president of the Photoshop users group in San Diego. "Artists don't like to be limited in what they can do with their tools. Let the U.S. government or whoever is involved deal with this, but don't take the powers of the government and place them into a commercial software package."

11/3/2008

Connor said the company's decision to use the technology was "not a step down the road towards Adobe becoming Big Brother."

Adobe said the technology slows its software's performance "just a fraction of a second" and urged customers to report unexpected glitches. It said there may be room for improvement.

The technology was designed recently by the Central Bank Counterfeit Deterrence Group, a consortium of 27 central banks in the United States, England, Japan, Canada and across the European Union, where there already is a formal proposal to require all software companies to include similar anti-counterfeit technology.

"The industry has been very open to understanding the nature of the problem," said Richard Wall, the Bank of Canada's representative to the counterfeit deterrence group. "We're very happy with the response."

Some policy experts were divided on the technology. Bruce Schneier, an expert on security and privacy, praised the anti-counterfeit technology.

Another security expert, Gene Spafford of Purdue University, said Adobe should have notified its customers prominently. He wondered how closely Adobe was permitted to study the technology's inner-workings to ensure it was stable and performed as advertised.

"If I were the paranoid-conspiracy type, I would speculate that since it's not Adobe's software, what else is it doing?" Spafford said.

Haley Dawn

From: Eugenie.E.Foster@frb.gov
Sent: Thursday, September 23, 2004 4:51 PM
To: Haley Dawn

Here are the key messages.

Thanks,

Genie
Eugenie E. Foster

Board of Governors of the Federal Reserve System
Division of Reserve Bank Operations and Payment Systems

----- Forwarded by Eugenie E Foster/BOARD/FRS on 09/23/2004 04:50 PM -----

Eugenie E
Foster/BOARD/FRS

09/20/2004 02:01
PM

David W Skidmore/BOARD/FRS

Michael Lambert/BOARD/FRS@BOARD

To

cc

Subject

Hi Dave,

Here is the language that I sent to my colleagues from the Central Bank Counterfeit Deterrence Group.

1. Manufacturers are working voluntarily with central banks to deploy technology that will protect their customers and other members of the public from counterfeit notes. The Federal Reserve and other central banks appreciate the manufacturers' voluntary support.
2. The central banks' counterfeit deterrence system does only one thing: it makes it harder for users to counterfeit currency. It does not compromise users' privacy by tracking their computer use, or by compiling or maintaining any information about them. The CDS does not affect their computers' performance in any way that they would notice, and it does not cost them anything.
3. The public can download images of new notes from the Bureau of Engraving and Printing's website.

Thanks,

Genie

Eugenie E. Foster

Board of Governors of the Federal Reserve System
Division of Reserve Bank Operations and Payment Systems

26 January 2004

Government Computer News

5

ISSN: 0738-4300; Volume 23; Issue 2

English

Copyright 2004 Gale Group Inc. All rights reserved.

With digital technology making currency counterfeiting easier than ever, the Federal Reserve is helping international bankers develop software to combat illegal money creation.

The Central Bank Counterfeit Deterrence Group, made up of Federal Reserve banks and the central banks of other G-10 nations, has released its code free of charge to the digital-imaging industry, Fed spokeswoman Susan Stawick said.

The deterrence software made its debut in October in Adobe Photoshop CS, said Russell Brady, a spokesman for Adobe Systems Inc.

An update of the Adobe Photoshop informational Web pages will explain the anticounterfeit feature and direct users to www.rulesforuse.org, a portal describing reproduction laws for the world's major currencies.

The Fed allocated \$2.9 million in fiscal 2003 for counterfeiting deterrence research, according to a budget document on the board's Web site.

COPYRIGHT 2004 Washingtonpost Newsweek Interactive

Central banks hope free software will put a dent in counterfeiting
top/haut

Effort to thwart crime shrouded in secrecy

PUBLICATION GLOBE AND MAIL

DATE: MON FEB.16,2004

PAGE: B3

BYLINE: KEVIN COX

CLASS: Report on Business

EDITION: Metro DATELINE: Halifax N

KEVIN COX

HALIFAX A group of central banks, including the Bank of Canada, are quietly giving secret anti-counterfeiting technology to computer and software manufacturers in an attempt to hinder hackers who try to print money at home. Officials with the RCMP and the Bank of Canada refuse to identify or discuss the technology because they don't want to tip off would-be counterfeiters about ways of thwarting the system. The system, which has been installed in many recent models of photo-imaging software and copying equipment, blocks computer users from downloading or printing digital images of many nations' currency -- including several Canadian denominations.

While the software use is now voluntary, there is a move in the European Union to draft legislation forcing the manufacturers of computer equipment to include anti-counterfeiting controls on any systems, scanners or printers sold in Europe.

The anti-counterfeiting software was developed by the Central Bank Counterfeit Deterrence Group, an organization of 27 central banks that includes Canada, Japan and the United States. The software is distributed free of charge to computer and software manufacturers.

Law enforcement agencies and banknote-issuing authorities around the world have been alarmed at the rise in digital counterfeiting as home computer operators are able to use scanners, laser printers and high-quality paper to produce difficult-to-detect bogus bucks.

According to RCMP statistics, the number of counterfeit bills circulating in Canada more than doubled from 2000 to 2002, with 208,457 bills circulating in 2002 compared with 94,133 in 2000. In the United States in 2001, police found that 608 counterfeit currency operations were using digital technology, compared with only 29 in 1995.

In Canada, it is a criminal offence to reproduce anything in the likeness of a bank note without the written permission of the Bank of Canada. However the Criminal Code specifies that no one will be convicted for

making a reproduction that is less than three-quarters or more than 1 1/2 times the length or width of the original bill. One-sided and black and white copies can also be made.

The counterfeit deterrence group has handed out its software to a growing number of technology companies for several years. However, Ginette Crew, spokeswoman for the Bank of Canada, said the organization would not discuss how many companies are using it or what systems have it.

"In the last few years the nature of counterfeiting has changed. Around the world we've seen an increase in counterfeiting rates attributed largely to cheaper computer technology," Ms. Crew said, adding that the central banks have asked hardware and software makers to include the anti-counterfeiting device.

Ms. Crew was not aware of any moves in Canada toward compelling manufacturers of computer equipment to include the anti-counterfeiting technology.

"We work with the hardware and software manufacturers to encourage them, but it's completely voluntary on their part as to whether they participate," Ms. Crew said.

The existence of the software only recently came to light when Adobe Systems Inc. of San Jose, Calif., acknowledged publicly that the counterfeit deterrence system was on their widely sold Photoshop CS imaging system.

But Ulead Systems Inc., the Taiwan-based maker of the PhotoImpact imaging system, has put the device in with its software for the past four years, Sharna Brockett, spokeswoman for the company, said in an interview.

She said Ulead put the counterfeit deterrence device on its photo-imaging software to ensure that it would not have any problems selling the system in the United States.

However, several Adobe Photoshop users were upset to discover that when they tried to open detailed images of banknotes they were greeted with an error message pointing them to a website containing currency reproduction regulations for several countries.

Adobe spokesman Russell Brady said the anti-counterfeiting system was installed in Photoshop at the request of the counterfeit deterrence group.

"We definitely think this [counterfeiting] is a serious business," Mr. Brady said in an interview. "With the widespread use of digital technology it has become far less expensive than it used to be and far more widespread, so we're sure counterfeiting by digital means is increasing."

Confidential

Draft

11/03/08

1

CDS

Basic statement about companies deploying CDS (the CBCDG counterfeit deterrence system)

The companies deploying the CDS agreed to this statement. No other comments should be made about any company.

A number of major manufacturers, including all major inkjet printer manufacturers in the world, have been working voluntarily with the Federal Reserve and the Treasury through the Central Bank Counterfeit Deterrence Group, a consortium of central banks, to deter the counterfeiting of currency by inkjet printers and personal computers. The manufacturers are phasing deterrence measures into their products over time. These measures do not violate any aspect of consumer privacy. This long-term program will be fully effective when the deterrence measures have become widely deployed.

Questions and Answers

Q: What is the counterfeit deterrence system (CDS)?

A: The counterfeit deterrence system is a machine-readable security feature that raises the cost, time, and visibility of using a PC to counterfeit a banknote. The security of Federal Reserve notes does not rely on any single security feature. Layers of machine-readable features secure Federal Reserve notes in combination with overt security features for public use.

Q: How will CDS technology work?

A: When a PC user attempts to copy a new \$20 Federal Reserve note the process will stop and the user will be referred to the "Know Your Money" website for information about reproducing Federal Reserve notes. The CDS is expected to prevent scanning, image editing, or printing of banknotes.

Q: Are all Federal Reserve notes protected by the CDS?

A: While we cannot comment on the specific features of future designs we would expect them to include features to deter PC counterfeits.

Q. If I cannot copy a new design note on my PC, how can I access a copy for allowable uses?

A: You can download authorized images of Federal Reserve notes from the website www.moneyfactory.com.

Q: What will be in my PC?

A: The counterfeit deterrence system employs technology that will interfere with the unauthorized reproduction of banknotes.

Q: Can this technology track my PC use?

A: The central banks developed the CDS to interfere with the capacity of personal computers to make unauthorized reproductions of currency images. The CDS will not track individual PC usage.

Q: Why did you select this particular solution?

A: An international group of experts evaluated the available technologies to deter PC counterfeiting and selected the CDS based on its easy incorporation into bank notes, application across the bank notes of many countries, and the potential for wide deployment in the PC industry.

Q: Is (Microsoft, Intel, Adobe, Compaq, HP, ...) supporting the system?

A: A number of companies are already supporting the system, and we expect more to do so. We do not disclose the identities of these companies.

Q: Are PC manufacturers the only companies supporting the system?

A: The central banks are looking to extend the system to all the devices commonly used for graphic imaging. The system targets both hardware and software devices.

Q: Are hardware and software companies readily supporting the system?

A: Many of the market leading companies recognize their responsibility to deter the use of their products in the counterfeiting of currency. Today millions of PC devices with CDS are deployed worldwide; by the end of 2003 the CBCDG expects there will be tens of millions of protected devices deployed. The central bank governors urge manufacturers and software developers to support deployment of this system.

Q: What is the Central Bank Counterfeit Deterrence Group?

Confidential

Draft

11/03/08

3

A: The Central Bank Counterfeit Deterrence Group was organized at the request of the Governors of the central banks of the G-10 countries to study counterfeiting threats to currency. The members include senior officials of the participating central banks, security specialists, and scientists.

Q: What countries are represented?

A: The G-10 central banks and those from a number of other countries are involved in this effort.

SC Marks

Q: What is it that prevents me from copying Federal Reserve notes on color copiers?

Q: Are the yellow numbers on the back of the note a security feature?

A: The Federal Reserve and the Treasury do not comment on the confidential features of Federal Reserve notes.

Haley Dawn

From: Eugenie.E.Foster@frb.gov
Sent: Friday, January 16, 2004 10:23 AM
To: Haley Dawn
Cc: Ferguson Tom
Subject: Re: This note is from [REDACTED]

----- Forwarded by Eugenie E Foster/BOARD/FRS on 01/16/2004 10:22 AM -----

Eugenie E Foster

01/16/2004 10:21
AM

To: robert.stone@bep.treas.gov
cc: Michael Lambert/BOARD/FRS@BOARD
Subject: Re: This note is from [REDACTED]

Bob:

Hope everything is ok with you.

Could you look into this Getty images website and let me know what it all means?

Thanks,

Genie

----- Forwarded by Eugenie E Foster/BOARD/FRS on 01/16/2004 10:20 AM -----

[REDACTED]@e.c
[REDACTED] >
om>
dawn.haley@bep.treas.gov, eugenie.e.foster@Frb.GOV,

To: [REDACTED]
cc: [REDACTED]

01/14/2004 01:54
PM

Subject: Re: This note is from [REDACTED]

Richard

Thanks. This is helpful, but it doesn't fully resolve my concerns. Right now, there's a lot of speculation and misinformation about exactly how restrictive the CDS technology is. I attached the URL for the Getty images Web site in my last e-mail because I really need to have an understanding of roughly what percentage of these types of images can still be created today using modern banknotes and CDS. How distorted, clipped, or small does a bill need to be before it can be opened in Photoshop without incident? I'd feel much better if I knew that CDS would only prevent images that are of a reasonable size and positioned more or less perpendicular to the line of sight. Any other images aren't really useful for counterfeiting purposes, so they really shouldn't be excluded. Is this a question that

Digimarc should address?

It's clear that more proactive communication from Adobe and the CBCDG is becoming necessary, or this issue is going to spiral out of control and begin affecting our sales--if it hasn't already. More importantly, the public perception of this is at risk of tarnishing our brand image, which we've worked very hard to maintain at a very high level. I'd like to be able to make some sort of public statement about the efforts the central banks are taking, as you've listed below, and what customers should do if they can't create or obtain the images they need. Will this be possible?

- Kevin

At 05:44 PM 1/14/2004 +0100, [REDACTED]

Kevin,

Sorry to respond a little late to your email messages of yesterday. As I indicated earlier, I'm attending an meeting in Europe and your messages only caught up with me this morning (this also accounts for the wrong email address). It appears that there is a bit more media interest following the AP story and I hope it's not causing you too much grief.

Firstly regarding your earlier email - please be assured that we are very comfortable with the positioning on the difficult questions you are receiving regarding work arounds. It is not the intention of the CDS to be a perfect barrier - it is intended to deter the casual or inadvertent copying of banknotes. The focus you placed on deterring youth and educating the public is exactly the right points to be making. Any vulnerabilities in the system are as a result of the trade-offs made to assure that the functionality and user experience is minimally affected. The central banks will not discuss the technical aspects of any implementation but will say if asked (and I was asked by AP but they didn't include it in the story) that Central Banks share the manufacturers' concern for minimising the impact of CDS on the user experience.

Regarding your later email, I'd like to address your concern's regarding the central bank's efforts to make images available to graphics professionals. As you know banknote reproduction legislation varies from country to country and the approaches by various central banks are different. As a result of the earlier conversation we had, a number of central banks have undertaken steps to assure that reproduction policy and the process for obtaining and using images within that policy aligns with the restrictions imposed by CDS.

The Bank of Canada is introducing a new policy this month that provides a means for images and permission for use to be obtained from the Bank. We are preparing a suite of images that can be used by graphic artist professionals which should be available when the policy is introduced.

The ECB has in place a restricted website available to professional (registered) users that provides high resolution banknote images for use by graphics professionals. They are planning to provide unmarked images on that site also.

In Japan the rules and legislation essentially prohibit the use of bank note images. (applicable legislation is fairly broad and reproduction is viewed generally as a potential offence). If you have specific feedback from Japanese users I would be happy to forward it to the Bank of Japan for their consideration.

The Swiss National Bank will make images available when in fact it becomes an issue in that country.

Following our previous discussion with the FRB and BEP a number of changes were made to the moneyfactory.com website, which I thought had addressed the concerns raised at the time. I've spoken with Genie Foster at the FRB and she would be happy to continue the discussion with you to determine the best approach to meet the needs of your customers and preserve the security of banknotes (I've copied her on this note). I think the best approach, when asked about the availability of images, is still to direct the questioner to the central bank for response. I hope that the above provides you with some confidence that central banks are acting to address the concerns regarding the availability of banknote images. If you feel it is useful, I'd be happy to talk with you directly when I'm back in the office Friday or organize a teleconference with the FRB, BEP and yourself for early next week. Of course, if you feel it would be helpful to have a face to face, I'm sure we could arrange to get the appropriate people out to your office on fairly short notice.

Kind Regards,
Richard

Any e-mail message from the European Central Bank (ECB) is sent in good faith but shall neither be binding nor construed as constituting a commitment by the ECB except where provided for in a written agreement.

This e-mail is intended only for the use of the recipient(s) named above. Any unauthorised disclosure, use or dissemination, either in whole or in part, is prohibited.

If you have received this e-mail in error, please notify the sender immediately via e-mail and delete this e-mail from your system.

Haley Dawn

From: [REDACTED]
Sent: Tuesday, January 13, 2004 5:36 PM
To: [REDACTED]
Cc: [REDACTED]; Haley Dawn
Subject: Concerns about CDS

Richard -

As I've become pulled into the current brouhaha over CDS, I've actually become concerned that the central banks may not be holding up their end of the bargain in terms of making it possible for graphics professionals to use currency images--within normal legal boundaries--just as they always have. For example, the only images available from moneyfactory.com have the words "specimen" emblazoned across them, which means they're not very useful for advertising purposes.

As you're well aware, money is a very powerful image in advertising and marketing, and it's hard to manage without it. I did a quick search on the Getty Images web site to find all of the images they have featuring paper money. I got a list of almost 3,000 images on 48 pages. You can see this for yourself at the link below:

<http://creative.gettyimages.com/source/search/resultsmain.asp?source=quickSearch&brand=allbrands&selImageType=7&chkLicensed=on&chkRoyaltyFree=on&txtSearch=paper+money&subSearch=Begin+search&UQR=gezxpj>

I suspect that it would be no problem to create many of these types of images even with the current CDS restrictions, because the images are probably too distorted or clipped to be detected. Not knowing how CDS works, however, I can't say for sure. More importantly, though, I spotted quite a few images that I suspect one might not be able to create any more, even though they're completely legal.

Can you respond to this? What exactly should the advertising and graphics community be doing in the future to get the proper images? I've been telling customers to contact their central bank, but, in all honesty, I'm starting to feel a little disingenuous giving that recommendation. I'm not convinced that they're going to be of help. Are my concerns valid?

- Kevin