Penn State International Law Review

Volume 16
Number 3 *Dickinson Journal of International Law*

Article 5

5-1-1998

The Consequences of Anonymous Access to the Financial Payment System

Richard T. Preiss

The Consequences of Anonymous Access to the Financial Payments System*

Richard T. Preiss**

I. Introduction

Rapid advances in technology have conferred vast benefits upon modern societies. Money can be wire transferred in an instant. The Internet has dispensed with the need to send faxes across telephone wires. The days when one was required to carry multiple currencies to travel across international borders have all but disappeared. The day is fast approaching when societies will be cashless and we will be able to carry so-called smart cards[1] that contain all of our funds in the form of electronic cash. Smart cards have the technical ability to facilitate transfers of electronic cash from one smart card to another. We can use electronic cash to shop on the Internet and even gamble there if we wish. The shares of a company could be bought and sold on multiple stock exchanges through electronic cash transactions. When the London stock

---

** Mr. Preiss has been an assistant district attorney in the Office of Robert M. Morgenthau, District Attorney of the County of New York, since 1980. Between 1980 and 1990, he prosecuted felony cases including homicide cases. In 1990, he was assigned to work on the investigation of the Bank of Credit and Commerce International with a team of prosecutors and investigators in Manhattan. Mr. Preiss recently completed a lengthy trial of three defendants prosecuted for international bank fraud in Manhattan. The views expressed in this paper are those of Mr. Preiss and do not necessarily represent the views of the Office of the District Attorney of the County of New York. The writer gratefully acknowledges the many helpful comments and suggestions of Joseph J. Dawson, Assistant District Attorney, Office of the District Attorney of the County of New York and Charles Rogovin, Professor of Law, Temple University School of Law (Philadelphia).

1. The term "smart card" as used in this paper means an electronic card with stored value in the form of electronic cash that can be used to access both national and international payment systems and to make point of sale transactions enabling its owner to purchase or sell goods and services, including electronic cash, without the use of physical cash or checks.

exchange is closed, for example, a person in the United Kingdom might transmit electronic cash to New York and buy publicly-traded shares because the stock exchanges in New York will be open. If a citizen of one country loses faith in the national currency, he might use an electronic cash transaction to convert his assets into the stronger currency of another country in a foreign bank account. The examples of how modern technology will continue to benefit us are numerous.

These benefits come with costs and present new challenges for law enforcement worldwide. One cost is that the new technology can be used to facilitate economic crime in both the domestic and international arenas. Criminals long ago learned that governments must observe borders, while criminals can ignore them with impunity.

This article begins with a description of an international bank fraud case that was tried in Manhattan and describes how traditional bank records enabled the prosecution to prove its case. It focuses on some of the issues that arise when modern technology is used by criminals and the challenges thereby presented to law enforcement. It also examines some of the consequences of payments systems that grant individuals anonymous access to those systems.[2] The article presents proposals for regulating the issuance and use of smart cards or any other stored cash value card available for general use in a financial payments system.[3] It concludes with the recommendation that anonymous access to any financial payments system for the payment or receipt of large amounts of funds should be barred to all individuals and institutions.

II. An Example of Bank Fraud

On February 19, 1997, a trial jury in Manhattan convicted three members of a family that operated banks in Puerto Rico, Panama, the Dominican Republic and Venezuela of various bank

2. The financial payments system includes both the domestic and international bank payments system and the ability to purchase or sell goods, services and currency.

3. An open payments system is one where the smart card or stored cash value card can be used anywhere to purchase or sell goods and services, including the ability to encode the smart card with electronic cash.

fraud and larceny charges. The writer was the lead prosecutor for this trial, which took more than three months to complete.[4]

A grand jury in Manhattan had indicted the three defendants[5] on evidence that millions of dollars had been stolen from their Puerto Rican bank and used to prop up two of their other banks. Further, the grand jury charged that the three defendants had schemed to defraud depositors of their Puerto Rican bank of millions more by misrepresenting both the quality of that bank where the deposits were supposed to be located and the very location of some of those deposits.

The crimes committed were truly international crimes. Most of the depositor-victims were Venezuelan nationals and few had ever set foot in Manhattan. Their money was supposedly placed in Puerto Rican and Panamanian banks; the deposits were funneled to Puerto Rico through New York and Miami banks. Virtually all of the money transfers were accomplished by means of electronic wire transfers or checks that were processed in Manhattan. Some of the money ultimately stolen was used to prop up Dominican and Venezuelan institutions.

Modern technology, albeit "low tech," assisted the Manhattan prosecutors in proving their case. Printouts from computers, microfilmed copies of account statements, checks, Swift messages, and the miracle of the copying machine allowed the prosecutors to show the jury exactly what had happened in the international and domestic bank payments system in Manhattan. In fact, the prosecutors were able to show that one of the defrauded depositors who lived in Venezuela opened a checking account at a Citibank branch a few blocks from the courthouse where the case was tried. That depositor used a check drawn on his account at that Citibank branch to open his account at the defendants' bank in Puerto Rico. Paper documents were available to trace the funds of that depositor and others through the banking system and to show the trial jury that the transactions actually took place in Manhattan and that the

4. The case was tried by three assistant district attorneys, Joseph J. Dawson, Jonathan E. Feigelson, and the writer. The names of the three defendants were Orlando Castro Llanes, Orlando Castro Castro, and Jorge Castro Barredo.

5. *People v. Castro et al.*, New York County Supreme Court Indictment Number 2459/96.

legal requirements of New York law had been satisfied.[6] Since it was all on paper for the jury to see, justice was done.

III. The Paperless Bank Fraud Case In Cyberspace

The prosecutors had a difficult time proving their case because, aside from certain transactions being processed in Manhattan, everything else took place in other jurisdictions, and the international bank payments system is quite complex and very difficult to understand. However, they had the documentary evidence and witnesses from New York financial institutions to prove that the transactions clearly attributable to the defendants' actions in Manhattan amounted to the thefts and obtaining of property from the various victims. While achieving a conviction was not an easy task, it is clear that in the cyberspace age it will be even more difficult to prove an international bank fraud case.

In cyberspace there will be no paper documents. There will be no account statements to help illuminate for a judge or jury what a prosecutor means when it is asserted that money went from Point A to Point B or from Person A to Person B. There may not even be bank accounts to prove the point that, when money is stolen or obtained by fraud from a person or business, it goes from one place to another.

In the coming age of smart cards and cashless societies, bank accounts, as they presently exist, may become obsolete. It is costly to acquire, process, and store paper, and it is expensive to retrieve. Indeed, those costs provide much of the motivation to dispense with paper in the first place. In the future, when a consumer needs only a computer and a secret code to pay his bills and move his money, he will have little incentive, and no inclination, to pay a bank to maintain records he already keeps on a hard drive or diskette at his home or office.

The day is fast approaching when anyone with money will be able to go to a street corner kiosk and purchase a form of swipe card encoded with electronic cash that can be used anywhere in the world. Already in New York City and other cities with mass transit systems, customers can go to a store or kiosk and purchase a Metrocard encoded with electronic cash that can be used to ride

---

6. The relevant statutes are the New York Criminal Procedure Law [§§ 20.20(1)(a) and 20.40(1)(a)] and the Penal Law [§ 20.00]. In essence, these statutes provide that if one element of a charged crime occurs within the state, New York courts have jurisdiction to hear the case and punish the offender in the event of a conviction.

the transit system. It is impossible to trace these cards because they can be purchased and used by anyone, without identification. It is only a short step from this scenario to one where consumers carry such cards for a range of purposes far wider in scope than riding trains. Future workers may be paid with electronic cash cards, instead of checks or wire transfers deposited into a bank account. What will stop drug dealers or fraudsters from placing ill-gotten gains on smart cards containing electronic cash and sending the cards out of the country? Such technology may very well eliminate the one advantage that law enforcement agencies now possess in the war against narco-launderers—the drug dealer's heavy burden of moving vast amounts of bulky currency across borders, or depositing those funds in bank accounts, without arousing suspicion. Clearly, advances in technology will lessen the criminals' burden of having to launder ill-gotten gains. Instead of lugging suitcases laden with currency onto an airplane, launderers will simply slip smart cards into shirt or skirt pockets and move vast sums with little effort or risk of detection.

How will law enforcement officials trace transactions on such cards when they have no bank account statements to examine? What will the prosecutors show the jurors and judges when bank fraud scenarios are repeated, as they surely will be? How will a prosecutor in any jurisdiction show the trier of fact that a financial transaction took place within the prosecutor's jurisdiction? How will any trier of fact be able to conceptualize an electronic transfer of funds if there is no paper to display and it is unclear where a transaction actually took place? Will electronic transactions be deemed to have taken place elsewhere from everywhere? When the effort is made by a prosecutor to pinpoint jurisdiction and venue, will the defense inevitably argue the transaction should be deemed to have taken place somewhere else?

IV. Smart Card Technology And Money Laundering Regulation

The national law of countries is very important in combatting international economic crime. A country whose laws do not keep up with changes in the international economy or that does not outlaw money laundering is virtually inviting criminal activity within its borders.

It is difficult enough for the law enforcement officials of individual countries with modern money laundering laws to stay abreast of technological developments and the benefits they confer upon criminals. The authorities are often too far behind the

criminals when it comes to technological sophistication. Add an international dimension to a case and there are even more obstacles to be confronted. The prosecutors in the Manhattan bank fraud case discussed earlier were fortunate because they received the cooperation of the foreign governments in those countries where critical evidence was found. Such, however, is not always the case and law enforcement officers often experience serious difficulties in obtaining evidence. If law enforcement agencies are having trouble now, it is not difficult to imagine what awaits if the smart card with its capacity to allow "purse to purse" transfers gains wide acceptance.

Like many other countries, the United States has enacted a comprehensive system of regulation designed to combat money laundering. The dominant regulatory weapon against money laundering in the United States is the Bank Secrecy Act.[7] It requires, *inter alia,* that financial institutions file a Currency Transaction Report (CTR) for cash transactions of more than ten thousand dollars within the United States.[8] It also requires anyone carrying more than ten thousand dollars in cash (including foreign currency) or any kind of financial instruments into or out of the United States to report that fact to the government at the border.[9]

In 1986 the United States Congress enacted the Anti Drug Abuse Act, which outlawed both money laundering[10] and the structuring of transactions for the purpose of evading the requirement to report currency dealings that exceed ten thousand dollars.[11] That Act was amended by the Drug Abuse Act of 1988 and strengthened the United States' effort to restrict money laundering.[12] It is fair to say that United States money laundering laws are the strictest in the world.

---

7. Amendments to the Federal Deposit Insurance Act Titles I and III, Pub. L. No. 91-508, 84 Stat. 1114-1124 (1970).

8. *Id.* at 31 U.S.C. §§ 5313 and 5324 (1988). The implementing regulations in 31 C.F.R § 103.11(g) define a financial institution very broadly. Moreover, 26 U.S.C. § 6050(I) generally requires persons engaged in a trade or business who do not come within the definitions of a financial institution to file the equivalent of a CTR with the government each time they engage in a transaction, or series of transactions, which involves more than ten thousand dollars in currency.

9. Bank Secrecy Act, at 31 U.S.C. § 5316.

10. The Money Laundering Control Act of 1986, Pub. L. No. 99-570, §§ 1351-1367, 100 Stat. 3207, 3218-39 (codified at 18 U.S.C §§ 1956-57) makes it a federal crime to launder proceeds from specified unlawful activity. Sections of the Money Laundering Control Act appear in 12, 18 and 31 of the United States Code.

11. 18 U.S.C. §§ 1956-57 (1987).

12. Pub. L. No. 100-690, 102 Stat. 4181 (1988).

The entire system of anti-money laundering legislation in the United States is premised on the notion that financial transactions will generate records that can be examined by law enforcement officials conducting a criminal investigation or prosecution. Those records might be in the form of paper or they might be stored in a computer, but they will be records of financial transactions nevertheless. Stated another way, the regulations place a name and other identifying information with a transaction and make it difficult for anyone to engage in large cash or cash-equivalent transactions within the bank payments system in an anonymous manner. United States money laundering laws make it more difficult, expensive and dangerous for criminals of all sorts to launder their profits. Criminals must go to extreme lengths to launder their monies.[13] They must use runners, corrupt accountants and other paid accomplices to assist them in laundering the cash they generate. And if they are apprehended by law enforcement, the penalties for violation of the money laundering laws are severe.[14] That said, and even without considering the advent of the electronic cash smart card, it is doubtful that law enforcement agencies in the United States uncover more than a small quantity of the money laundered in the United States. Notwithstanding the commitment of significant law enforcement resources, money

13. Recent events in New York City demonstrate the lengths to which drug dealers will go to launder their trafficking proceeds. A joint federal, state and city task force called the El Dorado Task Force, found that over $1.3 billion a year was being wire transferred to Colombia through storefront money service transmitters located in Queens, a borough of the City of New York. N.Y. NEWSDAY, June 23, 1997, at A3. Using 1990 census data, the Task Force determined that while the average immigrant family from Colombia earned $27,000.00 per year before taxes, the average Colombian family would have to send $50,000.00 a year to Colombia to account for the flow of $1.3 billion. *Id.* A Geographic Targeting Order (GTO) by the United States Treasury Department was issued that regulated the thousands of businesses that wire transfer money outside the United States. Statement of General Barry R. McCaffrey, Director, Office of National Drug Control Policy (March 11, 1997), Before the Subcomm. on General Oversight and Investigations, House Banking and Finance Committee. The GTO regulations required all New York money service businesses to report all cash wire transactions to Colombia over $750.00 (instead of the normal $10,000 threshold set forth in the federal money laundering statutes) and submit copies of picture identity cards of those involved. *Id.* Federal officials report that the Queens money service business dried up and seizures of smuggled cash at Kennedy Airport are up an astounding 900%. *Id.* While perhaps cynical, it is only a question of time before launderers find another way to move ill-gotten gains out of the country.

14. There are civil penalties for violation of the money laundering prohibitions along with criminal penalties including substantial fines and imprisonment for up to ten years if a violation is willful. 31 U.S.C § 5311 (1988).

laundering remains a major problem in the United States and other countries.

Assuming that the smart card attains widespread acceptance,[15] it will undermine the entire system of anti-money laundering regulation in the United States and those countries that have enacted similar record-sensitive legislation. Stated simply, there will be no records. The coming system of electronic cash and internet communication provides the money launderer with what he craves most—anonymity. Electronic cash cards will eliminate the record trail that law enforcement uses to apprehend money launderers. To whatever extent money laundering is a problem now, it will be far worse in the future age of electronic cash and anonymous Internet communication.

V. Proposed Solutions

The advent of the smart card means cheaper access to financial payment systems and elimination of the vast store of paper records inherent in the use of credit and debit cards and checks. With those advances, however, comes a more sinister problem. That is that smart cards will provide criminals with anonymous access to both domestic and international payment systems. It is that aspect of its utility that cries out for regulation by governments.

The writer has argued previously that those countries providing financial haven for the money launderers because of bank secrecy laws should be barred from the international bank payments system. Concerted action by the major industrialized countries of the world could achieve the necessary reforms.[16] In the smart card context, the argument is much the same—smart card and electronic cash issuers must not permit anonymous and untraceable access to any payments system, whether domestic or international,

---

15. It is not at all clear that the smart card will gain acceptance by the average consumer, although Mastercard is already advertising that its services include smart cards along with credit and debit cards. Most people who carry credit cards and bank debit cards do so for a very good reason—they do not wish to carry large amounts of cash with the attendant risk of loss. In its purest form, the smart card concept not only dispenses with physical cash, it also eliminates the need for a bank account and enables its owner to carry all of his assets, including his cash, on one small card in his wallet. It is at least questionable whether anyone would wish to risk the loss of everything in exchange for the ability to carry only one card and/or dispense with the need for a bank account.

16. Richard T. Preiss, *Privacy of Financial Information and Civil Rights Issues: The Implications for Investigating and Prosecuting International Economic Crime,* 14 DICK. J. INT'L L. 525, 539 (1996).

and appropriate pressures should be initiated to create such limitations—sooner rather than later.

The United States, for example, should not allow modern technology to undermine its comprehensive system of money laundering regulation. It should continue to bar anonymous access to the financial payment system by enacting appropriate legislation that requires at least the same sorts of identification that present laws require for the conduct of traditional financial transactions. That legislation should also apply the ten thousand dollar threshold-reporting requirement[17] for currency transactions to smart card electronic cash transactions. It should also consider lowering that threshold significantly if smart card technology gains wide acceptance. Finally, new legislation should prohibit "smart card to smart card" unrecorded transfers[18] of electronic cash that will not leave an audit trail. Failure to enact this kind of legislation virtually guarantees that the money launderers will take advantage of this new technology and undermine the present system of money laundering legislation.

No country is immune to the kinds of mischief that are sure to arise with the advent of unregulated smart cards and the absence of audit trails. The governments of the world have a shared interest in preventing the money launderer from doing his dirty business in anonymity, whether his activities abet drug dealing, fraud, theft or tax evasion. But the United States— whose citizens collectively constitute the world's largest consumer of narcotics—has the most incentive to battle money laundering and has the greatest interest in barring the use of any instrument or technology that provides money launderers with anonymous access to a financial payments system.

The United States should amend its bank regulatory and money laundering laws to eliminate the legal possession or use of any smart card that does not identify the user/owner of the card. This is hardly an unprecedented notion. For instance, we would never permit anyone to drive without first obtaining a driver's license issued in his or her name, containing an address, and often having a photograph as well. We should not allow anyone to "drive" into a public financial payments system without similar identification. Various scenarios come to mind.

---

17. *See supra* notes 9-11.

18. These are the so-called "purse to purse" transfers of electronic cash that allow the transfer of funds from one smart card to another.

The idea that anyone can approach a kiosk owner, give him huge amounts of cash and receive in exchange a card containing a corresponding amount of electronic cash is offensive. No industrialized country allows unidentified and unregulated persons to engage in banking activity. Certainly, a kiosk owner should not be permitted to act as a *de facto* banker with the power to convert paper money to electronic cash.

Some might suggest the best solution is a total ban on the use of smart cards. While that approach might have the virtue of simplicity, it hardly amounts to a fair or effective solution. After all, entire societies should not be foreclosed from using a convenient payment system merely because small but powerful criminal groups are likely to exploit and abuse one feature of that system. Simply put, one does not throw the baby out with the bath water; we must keep the child but clean the bathtub. The fundamental problem with electronic payment systems is the anonymity it provides to criminal users. The other features associated with these systems, including their built-in efficiencies, more than justify outright rejection of the notion that smart cards and electronic cash systems should be banned.

Others might suggest linking the card to some bank account within the jurisdiction where the card was issued or the card user resides. It is submitted that such a requirement comes close to the correct solution. This approach recognizes the virtues of smart cards but is narrowly tailored to meet the anonymity problem. Such a requirement would allow application of traditional "know your customer" rules to financial institutions that issue smart cards and provide records that could be used in a criminal investigation or prosecution.

Still another approach would be for governments to issue smart cards just as they issue currency, identity cards, passports, social security cards and taxpayer identification numbers. The cards issued could be electronically encoded at their point of issuance to the consumer with pedigree information for the user, including his name, address, social security number, and a password.

It is submitted that the best solution to the problem of anonymous entry into both domestic and international bank payments systems is a combination of the last two approaches discussed—linking smart cards to a bank account and requiring the issuing bank to maintain retrievable records of their use. The government would supervise their issuance—just as governments traditionally have supervised banking activity generally—by spot

check audits of both a bank's issuance and record keeping procedures.

The proposal here is to eliminate from commercial use any smart card issued by any business other than a bank. The issuing bank might charge a fee for issuing the smart card or the bank might issue the card for no charge to reflect the cost savings in not sending monthly statements to the customer as well as other paper handling costs. The market will determine the cost of smart cards. But the issuing bank would be required to maintain retrievable records of the smart card's use by the customer. If the cardholder desires a monthly statement, he can pay the bank a fee.

Before issuing a smart card, a bank would get to "know the customer" by requiring a personal meeting at the bank, examining the customer's documentation such as a driver's license, passport and other identifying documents and creating an electronically stored record of this information.

After issuing the smart card, the bank would keep a computerized record of all transactions on the card, including purchases of goods and services, the purchase of electronic cash, and deposits of electronic cash onto the smart card, with the date and location of those transactions.

Such a system has many advantages.

First, it will eliminate the law enforcement problem of anonymous issuance and use of the smart card. While it will still be possible to present false identity documents to obtain a smart card, it will be difficult, especially if photographic identification documents are required. Moreover, banks will keep a computerized and retrievable record of the smart card's use, something that banks now have the expertise to do and to do efficiently. A bank can simply scan the identity documents and store them in a computer to be retrieved when necessary. Thus when the money launderer, fraudster or thief uses the card to commit crime, the record will be available to support a prosecution.

Second, the proposal has the advantage of making the fraudulent use of the smart card more difficult. It is only a question of time before the fraudsters are able to produce fraudulent smart cards encoded with "counterfeit" identities and electronic cash, just as has been done with credit cards. With the flick of an electronic switch on a computer, these altered smart cards can be deactivated instantly as soon as they are inserted into an electronic terminal.

Third, traditional notions of financial privacy can be easily applied to the customer's records of purchases and use. The law

can continue to require that before law enforcement achieves access to an individual's smart card account, an appropriate subpoena or court order must be obtained.[19]

Fourth, a smart card's use can be monitored for suspicious account activity just as bank computers now monitor the traditional bank account for smurfing[20] and other nefarious activity. The computers can be programmed to monitor the smart card account and provide an alert that criminal conduct may be afoot. Present law already requires banks to alert law enforcement of suspicious activity in traditional bank accounts.

Fifth, the legal requirement that banks report cash transactions of more than ten thousand dollars to the government can be easily applied to electronic cash transactions in the same amount. Moreover, a smart card holder who takes cash in that amount into or out of the United States can be required by law to insert the smart card into an electronic terminal at the border before leaving or entering the United States just as an airline passenger must now present his passport under the same circumstances. A computerized and retrievable record of the electronic cash on the smart card will be created instantly.

Finally, the United States (and other countries as they see fit) should enact legislation that prohibits the use of any smart card that does not comply with the proposed legislation. The law should require that the domestic electronic terminals reject such non-qualified smart cards. After all, it would make no sense to impose these requirements for smart cards issued and operable in the United States only to have a non-complying smart card issued elsewhere used to access its financial payment system anonymously.

---

19. The United States has financial privacy laws that generally limit access by the government to an individual's account in a financial institution absent a court order. *See, e.g.*, 12 U.S.C. § 3402 (1995). A prosecutor must obtain a subpoena, either from a grand jury or from a court, and the financial institution must provide the demanded evidence under pain of contempt and its accompanying sanctions. *Id.* The prosecutor who obtains the evidence by grand jury subpoena is not permitted, and is indeed forbidden, to make public disclosure of such evidence unless authorized by law. *See, e.g.*, Fed. R. Crim. Proc. 6(e); N.Y. Crim. Proc. L. § 190.25(4) (providing that grand jury proceedings are secret); N.Y. Penal L. § 215.70 (providing that unlawful grand jury disclosure is a felony). If the prosecutor obtains a court subpoena calling for the production of the evidence, a protective order might be issued or a statute might limit what use can be made of the materials. *See, e.g.*, N.Y. Crim. Proc. L. § 240.50. That usually means the prosecutor may disclose it only in public court proceedings.

20. Smurfing is the structuring of a single currency transaction into multiple transactions of less than ten thousand dollars each to avoid a currency transaction reporting requirement. This practice is outlawed by 18 U.S.C. § 1956(a)(1).

After all, the United States has as much right to bar anonymous smart card holders from its financial payments system as does any country to regulate the conduct of persons present within its borders.

It is not suggested that adoption of these proposals will put an end to money laundering any more than has present money laundering legislation. Inevitably, criminals will find ways around any regulatory scheme and it will come as no surprise when criminals manage to corrupt smart card technology for their own purposes. Adoption of these proposals will, however, make it costly, difficult and dangerous for criminal organizations to use the financial payments system to launder their criminal proceeds. Furthermore, it will continue to give law enforcement at least a fighting chance to detect and prosecute criminal activity in the financial payments system.

VI. Conclusion

Governments cannot afford to make it any easier for the money launderer or criminals generally to dispose and make use of their ill-gotten gains. A smart card or stored value card that enables anyone to bypass the traditional, record-sensitive financial payments system will make it easier for criminals to do business, both domestically and internationally. Simply stated, legalized anonymous entry into or use of the financial payments system must never come to pass.

The proposal presented is a compromise representing a balance of competing interests. Banks seek to avoid the significant expense of maintaining paper records and strive to make the payments system more efficient. Their legitimate interest is to maximize profit by minimizing expense. Consumers, of course, have a legitimate interest in exploiting the convenience that smart cards can provide. Smart card issuers and retail merchants plainly have an interest in attending to the needs of consumers and profiting from their provision of these services. On the other hand, law enforcement agencies should not be forced to surrender one of the few advantages that they possess in the war against money laundering and crime generally: the availability and use of retrievable financial records for proof of criminal activity. The proposal set forth in this paper is a reasonable accommodation of competing interests, while continuing legitimate limitations upon criminal commerce in financial payment systems.