

July 19, 2002

Charles D. Klingman
Office of Consumer Affairs and Community Policy
Department of the Treasury
Room SC-37
1500 Pennsylvania Avenue, N.W.
Washington, DC 20220-0002

Dear Mr. Klingman:

The Mortgage Bankers Association of America (MBA), American Financial Services Association (AFSA) and Consumer Mortgage Coalition (CMC) appreciate the opportunity to provide the Treasury Department with some of our thoughts about issues raised by the Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56 (USA PATRIOT).

Title III of USA PATRIOT significantly amends the Bank Secrecy Act (BSA), which as you know applies among other financial institutions to a category called “loan and finance companies.” Under Sections 326 and 352 of USA PATRIOT, Treasury must for the first time propose BSA regulations for loan and finance companies, requiring the verification of the identity of persons opening new accounts and requiring loan and finance companies to institute anti-money laundering programs. Although institutions that might arguably fit the category of “loan and finance companies” – including lenders, loan brokers, loan servicers and investors in closed loans – might have little in common, and although it might be more appropriate not to write a one-size-fits-all regulation for the entire category, it appears that Treasury intends at least to propose rules covering the entire category. We welcome the chance to provide a perspective on the issues these proposed rules will cover that comes from a broad cross-section of institutions that may be considered “loan and finance companies.” In this letter we identify certain core issues that we hope Treasury can address in both of these regulatory areas, as well as discussing specific items of interest to Treasury. By considering USA PATRIOT regulations as an integrated whole, Treasury can have the greatest effectiveness at denying terrorists, drug dealers and other wrong-doers access to the American financial system – the overarching purpose of USA PATRIOT and our common goal.

We think that we can help provide such a broad perspective on money laundering issues. Our three organizations represent a significant portion of all of the institutions in the United States

that might be considered “loan and finance companies.” More importantly, our organizations represent an exceptionally diverse cross-section of the American financial services industry. MBA represents approximately 2,600 companies that engage in all aspects of real estate finance, including residential and commercial mortgage companies, mortgage brokers, commercial banks, savings associations, life insurance companies and other real estate-related financial service providers such as title companies, settlement attorneys and mortgage insurers. AFSA represents diversified financial services companies, automotive finance companies, consumer finance companies, mortgage companies, commercial finance companies, credit card issuers and merchandise and department store retailers with significant financial businesses. CMC represents some of the nation’s largest mortgage lenders, servicers and service providers, including both independent businesses and members of large, diversified financial services holding companies. In our day-to-day activities, we must reconcile the demands of many types of competitors, consumers and government entities. In responding to the challenge of terrorist infiltration with a broad perspective, therefore, we are suggesting an approach with which we are very familiar, and which we think has the greatest chance of being effective in the long run.

Our comments in this letter start with our understanding of the basic principles that the USA PATRIOT regulations must embrace. We go on to identify some of the special issues that Treasury should take into account in crafting verification-of-identity regulations applicable to lenders. We then discuss the aspects of the requirement to establish an anti-money laundering strategy that we think are of greatest concern to lenders. Finally, we consider the specific areas of money laundering concern that Treasury has identified in discussions with us over the last several months. We hope that our comments help you and your colleagues with the difficult task of writing regulations that strengthen the security of the American financial services industry without harming its exceptional vitality.

General Anti-Money Laundering Principles

We all agree that the primary goal of anti-money laundering regulations is to prevent terrorists and other money-launderers from using our financial system to harm us. In order to achieve this goal, we believe that three general principles must guide both the development of public policy and the implementation of anti-money laundering initiatives by individual financial services firms: (1) denial of access; (2) sustainability over the long term; and (3) coordination across the entire financial services industry.

Denial of Access

It is far easier to deny potential terrorists access to the financial system than it is to root them out after they have successfully achieved that access. This does not mean that we should only scrutinize persons seeking to open accounts or obtain new financial services. But it means that we should be most vigilant where our vigilance will do the most good: at the point of access to the financial system.

Sustainability Over the Long Term

To be effective, anti-money laundering efforts must be sustainable over the long term. This means any requirements must be *flexible*. Rigid obligations to report specific categories of transactions using specific forms submitted through specific channels become progressively less effective over time, as persons intent on evasion learn how to avoid triggering those obligations or providing reportable information. Giving financial institutions flexibility about what to track, investigate or report, by contrast, allows individual financial institutions to develop their own lists of “warning” signals appropriate to those institutions’ mix of businesses and customers – lists that institutions can modify as their business changes. We are encouraged that Treasury has so consistently mandated “risk-based” initiatives by financial institutions in its Section 326 and Section 352 regulations issued so far, and so consistently delegated the responsibility for determining the nature and extent of risks to individual financial institutions themselves. We think this strong commitment to flexibility should be maintained in future USA PATRIOT regulations.

These requirements must also be *institution-neutral*. Requirements that vary according to a financial institution’s technical legal status, rather than according to the activity the institution is performing, do little good and have destructive side-effects. They encourage evasion by setting up a hierarchy of institutions, some of which are subject to less stringent requirements than others and thus are more attractive to money-launderers. And over time they distort competition and increase inefficiency by imposing costly burdens on some institutions that other institutions in the same line of business do not share, and/or by encouraging the choice of a form of corporate organization according to the likely regulatory burden rather than transparent business considerations. Of course, the structure of the BSA, followed by USA PATRIOT, dictates that regulations will be institution-specific to a degree. But we encourage Treasury to avoid pitting institutions against one another as much as possible. We think it is important, for example, for Treasury to allow the reporting of all suspicious mortgage-related activities in the same way, with the same protections from potential liability, regardless of the legal category the reporting institution fits into. If banks are ever permitted to make such reports outside the SAR structure with BSA immunization, independent mortgage lenders should be given the same opportunity.

Finally, long-term sustainability requires that some consideration be paid to *costs and liabilities*. You have assured us that Treasury is aware of the costs of anti-money laundering activities and wants to avoid creating excessive burdens, and we are encouraged by Treasury’s consideration of this issue. But we nevertheless think it important to stress that obligations briefly undertaken in a crisis can become crushing if made permanent. This applies to the creation and implementation of security systems, the cost of which must not render uneconomic the activities that the systems are intended to make secure. This also applies to the incurring of contingent liabilities, which must not be allowed to overwhelm an institution trying to do the right thing. Thus, it should always be clear that a financial institution complying with appropriate anti-money laundering requirements – whether those involve mandatory reporting, voluntary

reporting based on its own risk assessments, denial of services at its own discretion, or other obligations –incurs no liability in connection with such compliance.

Coordination Across the Entire Financial Services Industry

We have also learned that a security system involving multiple participants must be coordinated to be effective. Every participant must know its own role and the roles of its fellow participants, and it must be able to rely on the other participants playing their roles.

In the financial services context, this means there should be *free communication between financial institutions*. Allowing financial institutions – all financial institutions, not just banks as in Treasury’s recent interim rule – to communicate directly with each other about nascent suspicions and known or potential threats dramatically improves all financial institutions’ effectiveness and the timeliness of their responses.

This also means there should be a *division of labor* within the financial services industry. Not all institutions have the same resources, technological capabilities or level of interaction with the customer. Allowing each segment of the financial services industry to contribute according to its unique strengths will increase the overall effectiveness of the industry at combating money-laundering. It also increases efficiency, by allowing the industry to use the resources that have already been developed rather than creating redundant new systems. For example, lenders such as our members already receive large amounts of information in connection with loan applications, particularly mortgage applications; it is appropriate that, to the degree that this information is considered valuable, lenders should be expected to collect, analyze and report it, where appropriate. To take another example, the money-center banks already track the origin and destination of payments using financial instruments such as checks and money orders; it is appropriate that, to the degree this information is considered valuable, the experts in collecting and analyzing this information be the ones to provide it.

This brings up a final point in connection with coordinating the financial services industry: that anti-money laundering obligations should always be *considered as a whole*. While regulations will have to be issued one-by-one, the specifics of an anti-money laundering strategy requirement can only make sense in light of the specifics of the due diligence an institution is required to undertake in connection with the opening of a new account, which affects the information that will be at the financial institution’s disposal in applying its anti-money laundering strategy and the timing of its activities.

Verification of Identity of Persons Opening Accounts

We therefore think it important to discuss our concerns about the requirement imposed by Section 326 of USA PATRIOT that:

The Secretary of the Treasury shall prescribe regulations setting forth the minimum standards for financial institutions and their

customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution[.]

Our concerns fall into four categories: when these standards should apply, what information should be scrutinized, who should be looking at the information, and who should retain the information.

When Should Minimum Standards Apply?

Section 326 requires that minimum standards established by regulation should apply “in connection with the opening of an account.” We think the obvious intent of this phrase is that the minimum standards should apply to all persons who actually obtain a financial service from a financial institution, or who would obtain the financial service but for the fact that the information they must provide to comply with the minimum standards raises suspicions of money laundering. This is important for the regulations to make clear, in order to avoid some of the unfortunate consequences for lenders of a broader, looser conclusion about when the minimum standards should apply.¹

Unlike some other financial services, consumers shop for loans such as mortgages and home equity loans, often quite aggressively. In the process, they may provide some information to a number of lenders in connection with obtaining a pre-qualification or even completing a loan application – but they do not follow through on all of these pre-qualifications or applications. Requiring lenders to collect, verify, check against federal lists of suspected terrorists, and then retain information on every person inquiring about a loan product will inflate application costs, slow down the application process, create false suspicions based on incomplete information submitted by consumers who change their minds during the shopping process, and introduce significant computer and physical storage issues based on the requirement to retain identification information in lender systems. We therefore think it should be made clear that, with regard to loans and other credit accounts, the minimum standards should apply to loans actually made or credit lines activated, not to applications.

What Information Should the Minimum Standards Require?

Section 326 contemplates that a financial institution will obtain an irreducible minimum of information about each of its customers. Treasury’s recently released proposed Section 326 regulations suggest that, for bank customers, this irreducible minimum will consist of an

¹ We note in passing that this is a point that the Treasury’s recently released Section 326 regulations for banks do not make clear. On the one hand, the regulations apply to “accounts,” defined as “each formal banking or business relationship *established* to provide ongoing services, dealings or other financial transactions.” Proposed 31 C.F.R. 103.121(a)(1) (emphasis added). On the other hand, the regulations apply to “customers,” defined to include “any person *seeking* to open a new account[.]” Proposed 31 C.F.R. 103.121(a)(3)(i) (emphasis added).

individual's name, date of birth, place of residence, mailing address and taxpayer identification number (or equivalent if a non-individual or foreign customer). In connection with most loans this is a modest amount of information, and verifying this information by scrutinizing identity documents is not difficult at an in-person loan closing – although online lending will be faced with special challenges that we hope Treasury will address. This may not, of course, be true for other financial services, which is why we think anti-money laundering regulations should be product-by-product rather than institution-by-institution. In the absence of regulations that apply to loans regardless of the maker of the loan (or separate regulations for mortgage loans, auto loans, unsecured loans and so on), we think it critical that the standards imposed on loan and finance companies be the same as those imposed on banks under the proposed rule.

Who Should Scrutinize the Required Information?

Section 326 imposes an obligation on financial institutions to verify the identity of “their” customers. Assigning a customer to a particular financial institution, however, is not necessarily an easy task. Take the example of a mortgage loan: a mortgage broker may take the application information; the application file may go to a lender for approval; an automated underwriting service provided by Fannie Mae or Freddie Mac may make a *de facto* credit decision on the application; and the lender may have a flow agreement under which the loan has been effectively pre-sold to a secondary market purchaser, with the servicing sold to a non-affiliated mortgage servicer. It is wasteful to require all of the participants in this loan transaction to go through the same verification process – for example to require all of the participants to check the lists of suspected terrorists maintained by the Office of Foreign Assets Control when it could most efficiently be checked once as part of the automated underwriting service. But without clear guidance on who has the verification responsibility, or clear permission to delegate the verification responsibility by contract to one party or another, no participant feels comfortable relying on any other. For Treasury to provide such guidance or permission would be very helpful.

Who Should Retain the Required Information?

A final issue to consider is who is responsible for retaining verification information. Unlike deposit accounts, which generally stay with the same institution, many lenders sell to investors most, if not all, of the loans they make. For example, as many as 80% of mortgage loans travel through multiple origination, secondary market or servicing channels. While most of the interim holders of a mortgage keep archival copies of information in loan files, this information is not easily accessible. As a result, there is an open question whether lenders and subsequent holders of loans need to change their practices in order to comply with the information retention requirement of Section 326.

This uncertainty can be avoided without sacrificing the accessibility of verification information. In our industry, there is generally at least one accessible copy of all of the information on the borrower of any given loan. This loan file generally travels with either the servicing rights to a

loan or the investment in the loan itself. Any obligations relating to the retention or retrieval of required verification information in connection with a loan should explicitly be imposed on the current holder of the loan file, and explicitly be removed from the other persons who may once have had access to the information in the loan file. Again, a clear statement from Treasury on this point would be very helpful in dispelling uncertainty as to this record retention and retrieval responsibility.

Anti-Money Laundering Program Requirements

We are aware, of course, that verification of customer identity is only a part of the larger obligation on every financial institution to have an effective anti-money laundering strategy. Section 352 of USA PATRIOT specifies that such a program must at a minimum:

- include internal policies, procedures, and controls;
- designate a compliance officer to administer and oversee the program;
- provide for ongoing employee training; and
- include an independent audit function to test the program.

Section 352 does not, however, provide specifics about the content of such a program. We are encouraged that Treasury is working to provide those specifics in regulations appropriate to the particular characteristics of the various types of financial institutions subject to this requirement. As we noted above, however, we think industry-by-industry regulation makes less sense than activity-by-activity regulation. To use our own experience as an example, we are acutely aware of how different the activity of lending is from (say) the activity of administering a deposit account, and we are therefore anxious that lending be subject to anti-money laundering program requirements appropriate to lending, not to requirements appropriate to depository institutions.

Most lenders, particularly those making closed-end loans, are primarily concerned with two questions: who they are lending to, and whether payments are being made on time. The flow of customer information through the typical lender's business follows these two priorities. It involves the acquisition of a great deal of information at or before making the loan – far more information than is required under the Treasury's recently released Section 326 regulations – in order to assess the future creditworthiness of the customer. Thereafter, however, it involves virtually no information gathering unless and until the customer fails to make a scheduled payment on time and in full. Except as necessary to assess borrower creditworthiness, most lenders do not routinely collect significant information about non-problematic customer accounts.

Depository institutions present a sharp contrast to this picture. Of course, they are interested in who is opening a deposit account, but only to the extent that the person can demonstrate the availability of funds to open the account. But thereafter, unlike lenders, depository institutions want and need to know what the customer is doing at any given moment: what instruments are outstanding, what are awaiting clearing, what the account balance is, where it has been, where it

is going, who is writing checks, who they are writing checks to. A depository institution cannot operate deposit accounts without keeping track of this payment-system information or delegating it to another depository institution or clearing house.

This stark difference in the nature of their two businesses should mean that the anti-money laundering responsibilities of financial institutions engaged solely in lending and those of financial institutions engaged solely in administering deposit accounts differ dramatically. Lenders should be expected to scrutinize the large amounts of information they receive in connection with loan applications for suspicious activities or evidence of money laundering – but they should not be expected to scrutinize payment systems issues such as who is making a routine payment. Depository institutions should be expected to scrutinize the source, transmission medium and destination of funds – but they should not be expected to unearth background information about their customers.

An example may make this point more clear. The typical commercial mortgage lender obtains a significant amount of information about a company seeking to obtain a commercial mortgage, including information about the borrower's officers, directors, nominal owners and sometimes even beneficial owners. This is and has long been a part of the commercial loan underwriting process. Commercial mortgage lenders can comb this information for what Treasury deems important and take appropriate action – provided, of course, that Treasury makes clear what information it wants scrutinized (officers but not shareholders? parent companies but not affiliates? immediate parents but not ultimate parents?), and provided further that Treasury makes clear that the lender is immunized from liability for its scrutiny and reporting of such information. Alternatively, commercial mortgage lenders can scrutinize this information according to their own assessment of the risks associated with a particular type of lending, property or customer – again, so long as it is clear that the lender is immunized from liability if it undertakes the risk assessment in good faith and implements procedures that are effective at putting the risk assessment into practice. But just as commercial mortgage lenders rely on their banks to handle the flow of loan payments, so they are entitled to rely on their banks to handle the USA PATRIOT scrutiny of those payments: who is making them, where the money is coming from, whether there are indicia of suspicion associated with the payment stream itself.

The anti-money laundering requirements imposed on the different parts of the financial services industry should complement one another. Lenders know some information better than depository institutions, and vice versa. The two should be allowed to contribute to the national anti-money laundering initiative represented by USA PATRIOT according to their strengths.

Areas of Particular Concern to the Treasury Department

With this in mind, we would like to discuss the specific concerns that Treasury has expressed in connection with the activities of loan and finance companies. In conversations with us, you identified certain specific patterns of borrower behavior that Treasury is concerned may indicate money-laundering activity. The patterns you have identified are:

1. Cash at closing, monthly payments in cash or cash pay-offs;
2. Large principal curtailments of mortgages;
3. Payments by multiple money orders or cashier's checks in small denominations
4. Frequent loan refinancings; and
5. Frequent drawdown and repayment of home equity lines of credit.

These activities raise a number of specific issues for our members, which we would like to discuss in greater detail.

Cash Payments

We think it would be a misapplication of effort to impose requirements on lenders to track or report cash payments differently than financial institutions are already required to report them.

Take the typical mortgage lender as an example. Mortgage banking is not a cash business. When a loan is obtained to fund the purchase or construction of a home, cash (currency/coin) is not accepted from the borrower at the closing table. The borrower is instructed by the originating lender to bring good funds in the form of a cashier's check, bank check, wire or personal check (for smaller amounts/discrepancies), and the lender relies on the settlement agent to enforce that instruction. On the rare occasion that a borrower brings cash to the closing table contrary to instructions, the settlement agent may be in a position to question and report the transaction, but the mortgage lender is not.

Borrowers rarely use cash to make monthly mortgage payments. This may once have been the case, when mortgage lenders serviced their own loans through local offices that accepted payments in person. But today, the majority of mortgages are serviced through the centralized servicing operations of independent mortgage companies and mortgage subsidiaries of depository institutions. To the extent that a mortgage lender has a local office, it is usually an origination-only establishment that is not equipped to accept mortgage payments in any form. Most borrowers are thus not able to walk into a mortgage company "office" to make a payment. The remote nature of servicing operations, the risk of theft and the risk of lost payments all encourage borrowers not to send cash.

Even pay-offs very rarely involve cash. Most pay-offs result from sales of the mortgaged property or refinances and involve the use of a settlement agent. In approximately 96% of such closings, the lender being paid off receives a check drawn on the settlement agent's account. Occasionally the funds will be wired directly from the settlement agent's escrow account to the mortgage servicer. Cash is never transmitted. Although a mortgage servicer would accept a cash pay-off if made, because of reluctance to make the borrower incur additional interest costs

while the cash was being returned and replaced with a money instrument, the fact is that such an event virtually never happens.

In sum, the industry believes there is very little risk of terrorists laundering cash through loan and finance companies. To the extent a borrower does use cash, we believe the current Currency Transaction Reporting requirements are adequate for the rare circumstances where such use runs a risk of money laundering.

Large Principal Curtailments

Treasury has expressed a concern that terrorists could launder money by financing the purchase of a property and promptly repaying the loan, then liberating funds by selling the property for cash or re-mortgaging it. This is a two-step process, and we note that, unless the property is sold for cash to a private person who does not finance the purchase with a mortgage loan, a mortgage lender will subject at least one party to the subsequent transaction to additional scrutiny in the mortgage loan underwriting process. In fact, if the terrorist attempts to obtain a cash-out loan, he or she will be attempting to obtain the mortgage product for which the additional scrutiny is most intense, and the likelihood of a transaction raising suspicions the greatest. We therefore do not think that large principal curtailments necessarily avail money launderers very much.

We must also note that principal curtailments are very common, and in our experience generally not an indicator of suspicious activity. Lenders incur a staggering number of principal curtailments each year, and it will be difficult for them to cull out "suspicious" transactions. The chart below compiles information gathered from four large mortgage servicers on the number of curtailments received last year (2001):

INFORMAL SURVEY OF FOUR MORTGAGE SERVICERS

| <u>Dollar Amount of Principal Curtailments</u> (excludes full pay offs) | <u>Number of Curtailments</u> <u>(last 12 months)</u> |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------|
| \$0-5,000 curtailments | 6,559,759 |
| \$5,001 – 10,000 curtailments | 20,939 |
| \$10,001 – 20,000 | 9,397 |
| \$20,001 + | 18,987 |
| Total Principal Curtailments in last twelve months | 6,609,082 |
| <i>Total loans serviced by surveyed lenders as of May, 2002</i> | 5,144,894 |

The loans captured by this survey represent approximately 13% of the estimated 40 million loans outstanding.² Extrapolating the data to the remainder of the industry results in an estimated 51.2 million principal curtailments made each year. Extrapolating from these numbers, it appears that about 160,000 principal curtailments in the United States per year involve sums greater than \$20,000. Lenders would have to employ significant resources to comply with a regulation that would call for further investigation or reporting of principal curtailments, especially if the reporting threshold were relatively low. The end result of such a requirement could well be to frustrate any monitoring system with large numbers of “false positives.”

Moreover, based on discussions between MBA and its members on the impact of treating principal curtailments as generally suspicious – which would trigger further investigation, information maintenance, or voluntary reporting to Treasury – we believe such treatment could overwhelm existing mortgage servicing resources in addition to relaying excessive and unnecessary information. We therefore think that a more nuanced approach is necessary, involving the identification and reporting of large principal curtailments that an institution regards as suspicious. Small curtailments and regular curtailments such as biweekly repayment plans should not trigger suspicion of money laundering.³ And, as we have noted above in stressing the flexibility that any anti-money laundering strategy needs to have to be workable, we think the line between large and small curtailments is one that institutions themselves should draw, and the indicia of suspicion should be ones selected by the institutions themselves, on the basis of their knowledge of their own business and customer mix.

As a final comment on this point, we note that certain items of information, while desirable to obtain, may not be obtainable from mortgage lenders and servicers. At this time, most mortgage companies do not have the technology to trend their customers’ payment behavior, making any further breakdown of prepayment information difficult. For example, it may not be feasible for lenders to determine if a borrower repeatedly makes large principal curtailments after the receipt of annual bonuses. This information may be more feasible to obtain from the depository institutions that handle borrowers’ deposits and payments.

Nonstandard Payment Instruments

Treasury’s third concern was that lenders might receive multiple payment instruments that would escape reporting by money services and depository institutions because of their small denominations. Treasury questioned whether loan servicers track the receipt of money orders, travelers’ checks, bank checks, or cashier’s checks. As noted above, this has never been a primary concern of lenders, and loan servicing systems have been set up without attention to the

² 1999 American Housing Survey.

³ A biweekly repayment plan results in the equivalent of one additional monthly mortgage payment a year, shortening the 30-year life of a traditional mortgage by approximately 7 years.

issue of the source of a loan payment. Few mortgage servicers, for example, identify and track what type of money instrument is received from the borrower because it is not critical to the servicing operation. Moreover, it is unclear whether lenders have the ability to identify the form of payment, apply the information to each borrower and track payment patterns. The highly automated function of processing mortgage payments creates a number of constraints. As mortgage volume has increased and servicing has concentrated into the hands of a few companies, the ability to manually accept and process payment is no longer possible. With the largest mortgage servicers processing over 5 million payments a month each, they are no longer able to visually inspect the payments they receive. Therefore, any effort to identify a money order or cashier's check would have to be automated.

Mortgage bankers must rely on third party lock box providers to process these payments. The lock box function is highly automated and involves the mechanical opening of mail, extraction of the coupon and payment, imaging of the money instruments, batching and depositing of checks at the mortgage company's bank, and posting to the borrowers' accounts. Human hands are rarely involved in this process. Although money instruments are imaged, the servicer does not view the items unless a specific problem arises with that payment.

At this time we are unable to assess the lockbox industry's ability to perform the identification and tracking functions you may be seeking. While depository institutions provide lockbox services to some loan and finance companies, and while those services may therefore already be subject to tracking requirements, other lockbox providers are independent and have not developed tracking capabilities. Our members report that lockbox providers vary widely in their technological sophistication, capabilities and flexibility. It may therefore simply be impossible at this time for lenders to comply with any absolute requirement from Treasury to identify and track so called "structuring" activities that involve the use of multiple small money orders, travelers' checks, or cashier's checks or other bank checks to make large payments.

Tracking Multiple Refinances

Treasury identified multiple refinances as a potential "red flag." We assume that Treasury is concerned about "cash-out" refinances of secured loans such as mortgages, as we do not see the special money laundering potential in a straight rate-and-term refinance of an existing debt or a debt-consolidation loan. Because borrowers shop aggressively for refinance loans, and because the market is extremely competitive, a borrower often refinances with a lender other than the one from whom the borrower obtained the loan being refinanced. As a result, lenders generally do not know how many times a particular debt may have been refinanced.

In some situations, this information may be available. When a mortgage loan refinances a previous mortgage loan, the land records will show some information about that transaction, and the land records may therefore reflect a pattern of multiple mortgage refinancings. Title companies, on which mortgage lenders rely for their title work, may therefore be able to flag suspicious chains of mortgage refinancings if given specific guidance as to what constitutes a

suspicious title record. Treasury may wish to take this possibility into consideration in writing the regulations that it must eventually write for “persons involved in real estate closings and settlements.” 31 U.S.C. 5312(a)(2)(U). In doing so, however, it should try to preserve the substantial improvements that have been made over time in the streamlining of real estate closings and the consequent reduction of closing costs. Title companies generally undertake abbreviated title examinations dating back only to the last mortgage on a particular property unless specifically requested to go back farther at additional cost and expense. And in any event Treasury should keep in mind that mortgage lenders, which themselves do not generally examine land records, are in no position to evaluate title records for suspicious activities.

In other situations, this information simply does not exist if the borrower does not (a) refinance with the same lender that provided the initial loan or series of loans, or (b) voluntarily disclose a chain of refinancings. In either of these cases, lenders are of course happy to monitor and report activities that Treasury specifically identifies as suspicious, but Treasury should be aware that most of this information resides solely with the borrower.

Use of Home Equity Lines of Credit

Finally, Treasury identified as an area of potential concern the frequent drawdown and repayment of home equity lines of credit. We understand Treasury’s concern – that a potential terrorist could repay a drawn-down home equity line of credit (HELOC) with funds received from a terrorist organization abroad, or that another type of money launderer could use suspect funds to repay the HELOC. This, however, is a question of the source of payment – which, as we have noted above, is more properly addressed to the financial institutions that operate the payment clearing and reconciliation systems. We are happy to cooperate with these financial institutions in any way we can, but we think it would be counterproductive for us to attempt to answer questions about HELOC payments that they are already equipped to answer but that we are not.

We also note that the capacity for frequent drawdown and repayment is intrinsic to HELOCs. Consumers with incomes that vary for nonsuspicious reasons, such as deriving a large portion of income from bonuses or periodic commissions, may well draw down and repay their HELOCs “frequently” for the legitimate purpose of evening out household cash flow. We can and do screen HELOC applicants for their creditworthiness, which includes an evaluation of their likely future income, whether from regular income or periodic bonuses or commissions, and we are not likely to give a HELOC to a person who cannot demonstrate the likelihood of having legitimate income. We think this is the best protection against the use of HELOCs for money laundering purposes, and it is certainly the aspect of protection that our members are best capable of providing.

Charles D. Klingman
July 19, 2002
Page 14

Conclusion

As we hope this letter has made clear, we conceive of anti-money laundering regulations as a complex system in which each part of the financial services industry plays a unique role. For the reasons explained above, we think that the proper role of loan and finance companies in the war against terrorism is to deny potential terrorists – as well as other potential money launderers – access to the part of the U.S. financial system that we control. We think that our specific comments have outlined a method for denying access that is both sustainable over the long term and coordinated with the proper roles of the other parts of the financial services industry.

We would be happy to discuss in greater detail any of the issues raised in this letter. Please contact any of: Vicki Vidal, Senior Director, Government Affairs, Mortgage Bankers Association of America (202 557-2861); Monique Gaw, Vice President, Federal Government Relations, American Financial Services Association (202-296-5544); Anne C. Canfield, Executive Director, Consumer Mortgage Coalition (202 544-3550).

Very truly yours,

MORTGAGE BANKERS ASSOCIATION OF AMERICA

AMERICAN FINANCIAL SERVICES ASSOCIATION

CONSUMER MORTGAGE COALITION