HOUSEHOLD

Credit Card Services
2700 Sanders Road
Prospect Heights, IL 60070

847 564 5000 Telephone
847 205 7417 Facsimile

Via Hand Delivery

March 29,2002

Office of the Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW
Room 159
Washington, DC 20580

Re: Telemarketing Rulemaking – Comment
FTC File No. R411001

Dear Sir:

We appreciate the opportunity to submit this comment to the Notice of Proposed Rule Making ("Proposal") published by the Federal Trade Commission ("Commission") to amend the Commission's Telemarketing Sales Rule ("Rule"). Household Bank (SB), **N.A.** and Household Bank (Nevada), **N.A** (collectively "Household") are two of the largest issuers of MasterCard and VISA credit cards in the United States. Household's principal bank card programs are the GM Card, a co-branded product offered in conjunction with General Motors, and the Union Privilege credit card program, an affinity program offered in conjunction with the AFL-CIO. In addition, through its Household Bank and Orchard **Bank** branded programs, Household offers credit cards to middle-market Americans underserved by traditional credit card providers. Household makes its credit card products available via mail, telephone, the internet and partnership marketing. Household manages over $17 billion in credit card receivables and its customer base totals over 15 million. Household's credit cards are serviced by its affiliates, Household Credit Services, Inc. and Household Credit Services (11), Inc. which together employ over 5000 men and women throughout the country.

General

Telemarketing is a valuable tool that enables legitimate businesses to offer goods and services to consumers in a cost effective and efficient manner. Consumers, and ultimately the economy, benefit from this method of marketing in a number of ways, including the increased availability of low cost goods and services, a wider variety of choices, and the convenience of shopping nationwide and effecting a purchase in the comfort of their own home. For these reasons, Household supports the efforts of the Commission to curtail telemarketing fraud and

abuse in accordance with its authority under the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 (the "Act"). As further discussed below, however, we are concerned that in trying to address the abusive practices of unscrupulous telemarketers, the Commission has included a number of provisions in its Proposal which will negatively impact the ability of legitimate businesses to reach their own customers, as well as other consumers who may want or need their goods and services.

As discussed in greater detail below, we have significant concerns with respect the do-not-call provisions of the Proposal (§310.4(b)(1)(iii)(B)). First and foremost, the Commission's proposed do-not-call provisions do not exempt calls made to existing customers. In addition, the provisions would, in effect, create an additional do-not-call list that would be layered on to an already complicated and inconsistent patchwork of state do-not-call laws. We are also concerned with the provisions of the Proposal that would restrict the sharing of billing information (§ 310.3(a)(3) and § 310.4(a)(5)) and instead require consumers to disclose their account numbers to telemarketers. This requirement is contrary to the longstanding advice against this practice given by the Commission and the financial services industry. (See e.g., attached brochure issued by the Office of the Comptroller of the Currency ("OCC") entitled "How to Avoid Becoming a Victim of Identity Theft" and Section VI of OCC Advisory Letter **AL** 2001-4.) Further, the information sharing restrictions of these sections would conflict with the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) ("GLBA") and the Commission's own regulations implementing that law. 16 C.F.R. Part 313. While the GLBA was enacted after the Commission completed its review of the Rule, any final rule adopted by the Commission should acknowledge that the sharing of billing information between a financial institution and a third party telemarketer is governed exclusively by the GLBA and, in the case of an affiliate, by the Fair Credit Reporting Act (15 U.S.C. §16.81 et seq.) ("FCRA").

For these reasons and as discussed further below, we urge the Commission to continue its careful consideration of revisions to the Rule and refrain from issuing final revisions until it has published a revised proposal for public comment.

Definition of "Billing information" (§ 310.2(c))

In order to avoid conflict with the GLBA, we suggest that the definition of "billing infomation" be clarified to exclude encrypted account numbers where the means to decode the encryption are not provided to the recipient. This clarification would be consistent with the Commission's interpretation of the GLBA wherein it stated that it "believes an encrypted account number without the key is something different from the number itself...". 65 Fed. Reg. 33646, 33669 (2000). Rather, the Commission continued, "[an encrypted account number] operates as an identifier attached to an account for internal tracking purposes only." Id. In further interpreting the meaning of "account number", the Commission referenced the concerns of commenters that "if internal identifiers may not be used, a consumer would need to provide an account number...which would expose the consumer to a greater risk than would the use of an

internal tracking system that preserves the confidentiality of an account number that may be used to access the account." Id. The Commission concluded that "[c]onsumers will be adequately protected by disclosures of encrypted account numbers that do not enable the recipient to access the consumer's account." Id. These conclusions should apply equally with respect to the Proposal.

While the specific language of the proposed definition of "billing information" appears consistent with the Commission's interpretation under the GLBA, our concerns arise from the Commission's discussion of the term in the Supplementary Information to the Proposal. Specifically, the Commission states that it intends "billing information" to include "information such as a credit or debit card number and expiration date....customer's date of birth or mother's maiden name, and any other information used as proof of authorization to effect a charge against a person's account". 67 Fed. Reg. 4492,4499 (2002). This appears to go well beyond the Commission's specific language defining the term as "data that provides ***access*** to a consumer's account" (emphasis added) and, as used in proposed section 310.4(a)(5), conflicts with the sharing of encrypted account numbers and, subject to a consumer's right to opt-out, the sharing of other non-public personal information as permitted by GLBA. To avoid such a conflict, we suggest that the Commission clarify that the term "billing information" includes only account numbers, and specifically excludes encrypted account numbers where the method for decoding the encryption is not provided to the recipient.

Definition of "Outbound telephone call" (§ 310.2(t))

Also, of significant concern to Household is the Proposal's definition of an "outbound telephone call" *to* include certain calls initiated by a consumer. Thus, if a consumer decides to contact a company by telephone to inquire about a product, and after purchasing the initial product is offered a second product by the same telemarketer but on behalf of a different seller (e.g., an affiliated company) or "is transferred to a telemarketer other than the original telemarketer," the second part of the call appears to be subject to the restrictions of the Rule that apply to "outbound telephone calls." These restrictions include the limitation on contacting customers who have gut themselves on the do-not-call registry (proposed section 310.4(b)(1)(iii)(B)), the restrictions on what time an outbound telephone call may be made (section 310.4(c)), and the making of required disclosures (section 310.4(d)). This proposed change, though well-intentioned, would create an unworkable standard that is neither justified by the concerns raised in the Preamble nor authorized by statute.

The Act specifically authorizes the Commission to issue rules to protect against "deceptive telemarketing acts or practices and other abusive telemarketing acts or practices," not telephone calls in general (15 U.S.C. 6102(a)(1)). Most notably, the only times the Act discusses "telephone calls," it specifies "unsolicited telephone calls" or calls made by the telemarketer "to the person receiving the call" (15 U.S.C. 6102(a)(3)). The Act lacks any indication that Congress intended the Commission to regulate anything but outbound calls (in the sense meant

by the Rule), and there is no alternative authority for the Commission's proposed expansion of the Rule to apply to inbound calls.

Even if the Commission has the authority to issue the proposed changes, the new definition as proposed is not tailored to the problems it is intended to address. The Commission states that it has proposed this change to the definition of an outbound telephone call in response to a reported increase in the practice of "up-selling." 67 Fed. Reg. 4492,4500. Moreover, the Commission specifically highlights the problems that arise when "up-selling" occurs after a consumer has provided a telemarketer with billing information and has closed a sale. 67 Fed. Reg. 4492, 4495. However, the new definition would bring numerous situations within the scope of the Rule that do not pose the risks the Commission has stated that it is trying to address, as the new definition of "outbound telephone call" is not limited to situations where billing information has been provided, nor to those where a sale has been made.

The result of attempting to force inbound calls to fit the regulatory model created for outbound calls is to create unjustifiable and, in some cases, absurd consequences. For example, if a consumer initiates a call to a business and is put on hold, and the recorded message playing during the hold period urges the consumer to consider purchasing various products or services, the Proposal would appear to require the call to be treated as an outbound telephone call. If the consumer initiated such a call before 8 a.m. or after 9 p.m., the call would then be an outbound telephone call at an impermissible time and ***per*** se abusive – despite the fact that the consumer would have chosen the time of the call, and presumably would only have called at a time the consumer herself found acceptable. Moreover, the telemarketer may not even know what time it was in the consumer's jurisdiction when the call was placed. Meanwhile, if the caller had registered on the do-not-call registry, the second telemarketer could be violating proposed section 310.4(b)(1)(iii)(B) even though the telemarketer did not call the consumer and has no practical way to determine whether the consumer is on that list. There is simply no reasonable basis for treating any call the consumer has initiated, at a time and to a recipient of the consumer's choosing, as ever being subject to the same panoply of limitations as a call over which the consumer has no such control. In light of these weaknesses in the Proposal, we suggest that the definition of "outbound telephone call" in the Rule not be altered.

Consumer initiated or inbound telemarketing calls have been in general use well pnor to 1994 and the passing of the Act and the Rule. Indeed, the Rule exempts inbound calls for logical reasons. What makes an inbound call different from an outbound call is that it is initiated by a consumer who calls to purchase goods and services and directly provides (during the call) his or her billing information for that purpose thereby employing what the FTC has characterized as "the most fundamental tool consumers have for controlling transactions, i.e., withholding the information necessary to effect payment unless and until they have consented to buy." 67 Fed. Reg. 4492,4496. "Up-selling", or offering the consumer an opportunity to purchase other goods and services after the initial purchase is completed, preserves the highest level of consumer protection because the consumer is specifically asked and consents to the additional goods or

services being charged to the same billing source the consumer provided moments before. If the true concern of the Commission is that the original or second telemarketer provides the required disclosures to the consumer, this can be achieved without creating the paradox of an inbound call becoming an outbound call.

It is also worthwhile to note that, contrary to the implicit assumption in the Proposal that all "up-selling" is bad for consumers, there exist "up-selling" opportunities that provide significant benefits to consumers. Numerous examples of these exist in the consumer credit industry, and telemarketing provides an important opportunity for financial services providers to provide consumers with information on products they may qualify for, need, that may save them money, and that they may not have otherwise heard about. Examples of products that are "up-sold" include – consolidation loans to reduce higher rate debt, automatic payment plans that may qualify customers for savings on their loan payments, debt cancellation programs that may protect a borrower in the event of unemployment or disability, and reduced rate loan products for customers of affiliated financial institutions. Many of these products, as well as many other financial products, are sold by separate companies that are either commonly owned or that have agreed to offer products to each other's customers. Unduly restricting the financial services industry from offering such products to callers who have, of their own volition, contacted them, is wholly beyond the scope of the Act and unrelated to the "up-selling" threat enumerated by the Commission.

Restrictions on Submitting Billing Information (§ 310.3(a)(3)

As it is currently drafted, the Rule requires telemarketers to obtain the "express verifiable consent" of the consumer before submitting the consumer's "demand draft or similar negotiable paper" as payment in a sales transaction. The Commission seeks to expand the express verifiable authorization requirement to cover any other method of payment where such method does not have the protections available to consumers under the Fair Credit Billing Act ("FCBA") and the Truth in Lending Act ("TILA"), as amended. We commend the Commission for recognizing that consumers are well protected under the provisions of the FCBA and TILA, and agree with the Commission that when using payment methods covered thereby, the express verifiable authorization requirements should not apply.

The Supplementary Information to the Proposal provides that methods of payment having protections "comparable to those available under" the FCBA and TILA would also be exempt from the express verifiable authorization requirements. 67 Fed. Reg. 4492,4506. Based on this language, we believe the Commission would also consider exempt from the express authorization requirements payment transactions which are subject to the Electronic Fund Transfer Act (15 U.S.C. §§ 1693 et seq.) ("EFTA") as its provides protections quite similar to those available under the Federal Reserve Board's Regulation Z, which implements the TILA and FCBA. Like Regulation Z, the Federal Reserve Board's Regulation E, which implements the EFTA, provides consumers with the opportunity to dispute any "errors", such as an unauthorized

electronic fund transfer, reflected on the consumer's billing statement. 12 C.F.R. § 205.11. Also, like Regulation Z, Regulation E generally limits the consumer's liability for unauthorized electronic transactions to $50. 12 C.F.R. § 205.6. For these reasons, we suggest that the Commission clarify that payment transactions covered by the EFTA would also be excluded from the express verifiable authorization provisions of this section.

The Commission also proposes to expand the list of information that must be received in order to deem a consumer's express oral authorization verifiable. Of significant concern to Household is the inclusion in this list of the consumer's account number. According to the Supplementary Information to the Proposal, the account number "must be recited by either the consumer or the telemarketer." 67 Fed. Reg. 4492,4506. On the one hand, this requirement is not workable when the account number pertains to an account held by a financial institution that is subject to the GLBA. Under the Commission's own rules implementing the GLBA, financial institutions are prohibited from disclosing account numbers to non-affiliated third parties for marketing purposes. 16 C.F.R. § 313.12. Consequently, in most instances a telemarketer will not have an account number to recite. And, in those situations where the GLBA does not apply, it is difficult to envision under what circumstances a telemarketer would come to possess an account number in the first place, given the Proposal's definition of "billing information" and the restrictions in proposed section 310.4(a)(5). The end result is that it would be the consumer, in most if not all cases, who would be required to place herself at risk by disclosing her account number. And not only is she disclosing it to the individual telemarketer she is speaking with on the telephone, but she is also disclosing it to any other party on the line who may be auditing the telephone call for quality control purposes, and any other person with whom either of those individuals choose to share her account number. It is for the express purpose of avoiding these risks that both the Commission and the financial services industry have long discouraged consumers from disclosing their account numbers to telemarketers.

Consumers are best protected where the financial institution, and not the telemarketer, controls access to the consumer's account. With this control, it is the financial institution that initiates charges to the consumer's account after it is satisfied that the telemarketer received the requisite authorization from the consumer to do so. This control, and the consumer protections that go along with it, are compromised by this provision of the Proposal. Therefore, we strongly urge the Commission to remove the consumer's account number from the list of information necessary to verify oral authorization. If for some reason the Commission decides to retain the account number requirement, then we respectfully request that it be eliminated for telemarketing situations where the GLBA applies.

Restrictions on Sharing Billing Information (§ 310.4(a)(5))

Here the Commission proposes to regulate the sharing of information which is clearly outside the scope of its authority under the Act. Congress directed the Commission to enact rules prohibiting abusive, deceptive, and fraudulent *telemarketing acts* (emphasis added).

According to the Supplementary Information to the Proposal, the practice that lead the Commission to propose this section is the misuse by telemarketers of billing information. Clearly, the abusive telemarketing act is not the sharing of the billing information in the first instance, but is the misuse of that information by unscrupulous telemarketers. Rather than specifically addressing that abusive act, however, the Proposal effectively prohibits any sharing of billing infomation at the expense of legitimate businesses and, ultimately, the consumer. Not only does this approach exceed the Commission's statutory authority, it is also directly conflicts with the GLBA and the Commission's regulations implementing the same. And, like section 310.3(a)(3) discussed above, this provision of the Proposal risks actually increasing the incidence of fraud against consumers who will now be encouraged to provide their account number over the telephone. For these reasons, the Commission should not include this section of the Proposal in the final rule. If the Commission chooses to retain this provision, then, at a minimum, we suggest it be clarified as explained below to remove all conflicts with the GLBA and preserve the intent of Congress, the Federal functional regulators ("Agencies"), and the Commission with respect thereto.

The extent to which this proposed section conflicts with the GLBA depends on whether information is being shared with the financial institution's affiliate or with a non-affiliated third party. It also depends on the definition of "billing information" as discussed previously and again below.

Pursuant to the FCRA, financial institutions are permitted to share account information with their affiliates and it is a common practice for financial institutions to share such information with affiliated companies that perform telemarketing services on the institution's behalf. If the account information is deemed to be credit information, it may only be shared with affiliates after the consumer to which the credit information relates has been given prior notice of the sharing, the opportunity to opt out of the sharing, and has not exercised that opt out right. As drafted, the Proposal conflicts with these FCRA information sharing provisions under which financial institutions have operated for years. In addition, the necessity of these amendments in the context of affiliate sharing is illusive. A financial institution's affiliate is certainly not going to **risk** harming that institution's customer relationship by engaging in the abusive actions the Proposal's provisions are intended to prevent. Therefore, if retained, section 310.4(a)(5) should be modified to except from its coverage the sharing of billing information between financial institutions and their affiliates.

As noted by the Commission in the Supplementary Information to the Proposal, financial institutions may also contract with third parties to telemarket their customers. **A** financial institution's sharing of information with such parties is governed by the provisions of the GLBA and its implementing regulations. See e.g., 16 C.F.R. Part 313. In passing the GLBA and drafting its implementing regulations, Congress, the Agencies, and the Commission, respectively, gave substantial consideration to the issue of information sharing by financial institutions with non-affiliated third parties. As the Commission is no doubt aware, subject to certain enumerated

exceptions, the GLBA prohibits financial institutions from sharing non-public personal information about consumers with non-affiliated third parties if, after giving a consumer notice and the right to opt out, the consumer elects to opt out of such sharing. However, a consumer's election not to opt of sharing under the GLBA would, effectively, be rendered moot by this proposed section based on the broad definition of the term "billing information". As previously discussed, this conflict can be avoided if the Commission clearly provides that "billing information" includes only unencrypted account numbers and excludes encrypted account numbers so long as the method to decode the encryption is not provided to the recipient.

The next conflict between this portion of the Proposal and the GLBA arises with respect to the sharing of account numbers themselves. The sharing of account numbers for marketing purposes is addressed separately from all other information sharing under the GLBA and its implementing regulations, illustrating the significant consideration already given to the issue by Congress, the Agencies, and the Commission, respectively. Under the GLBA, financial institutions are prohibited from sharing account numbers with any non-affiliated third party for marketing purposes, including telemarketing, with two specific exceptions. First, the financial institution is permitted to share account numbers with its agents or service providers that are marketing the financial institution's own products, so long as the agent or service provider is not able to directly initiate a charge to the related account. 16 C.F.R. § 313.12(b)(1). Second, financial institutions are allowed to share account numbers with their partners in private label, affinity or similar programs where the participants in the program have been identified to the consumer. 16 C.F.R. § 313.12(b)(2). These exceptions were adopted by the Agencies and the Commission because they are necessary for a financial institution to continue to engage in its legitimate day-to-day business and pose no significant risk to consumers. Therefore, if this proposed section 310.4(a)(5) is retained in the final rule, it must be amended to include the foregoing exceptions.

Finally, this proposed section raises the same significant concerns previously discussed with respect to the Commission's proposed requirement that consumers provide their account numbers over the telephone. Requiring the consumer to determine when to provide this information places the burden on her to distinguish the legitimate from the unscrupulous telemarketer. This will greatly increase the risk of fraud which harms both consumers and the financial services industry and is, of course, contrary to the purposes of the Act and the intentions of the Commission. As discussed above, this risk can be avoided by not requiring consumers to disclose their account numbers over the telephone and by not prohibiting the sharing of encrypted account numbers which, in promulgating the GLBA regulations, the Agencies and the Commission agreed poses no risk to a consumer, provided the key to decode the account number is not also provided to the recipient.

Other concerns raised by the Commission prompting this portion of the Proposal include consumers not knowing which account would be charged and how the telemarketer came to possess their account information. This concern can be alleviated more easily and without

increased risk to the consumer by disclosures, which legitimate telemarketers already provide, such as the brand name of the account being charged and the name of the entity from which the telemarketer received the encrypted account number.

We share the Commission's concern regarding unauthorized use of a consumer's billing information, as this practice harms both consumers and financial service providers. But, even assuming it is within its statutory authority to do so, by restricting a financial institution from sharing customer information with legitimate businesses with which it contracts, the Commission will inadvertently increase the risk of fraud against consumers and the financial services industry. In addition, such restrictions on a financial institution will negatively impact its ability to continue to make products and services available to consumers in a cost effective and efficient manner. The GLBA and its implementing regulations strike a balance between the protection of consumer interests in this regard and the continued flow of information for use by legitimate businesses. Given the fact that the GLBA regulations have been in effect for less than one year, it is certainly not necessary for the Commission or any other regulatory body to revisit and further restrict information sharing practices at this juncture. Therefore, if proposed section 310.4(a)(5) is retained in the final rule, we suggest the Commission clarify that its provisions are not applicable to financial institutions covered by the GLBA.

National Do-Not-Call Registry (§ 310.4(b)(1)(iii)(B)

Outbound Telephone Calls Made to Existing Customers

As a general matter, we support the concept of a national do-not-call list. We believe that when there is no existing business relationship between the consumer and the business making the telemarketing call, the interests of both can best be served by a simplified' and centralized method to record and communicate a consumer's telemarketing preferences. However, where there is an existing business relationship, we believe the least burdensome and most efficient method for the consumer to communicate and the company to honor her wishes in this regard continues to be the company specific approach as provided in the original Rule and the TCPA (47 U.S.C. 227 et seq.). For this reason and those set forth below, outbound telephone calls made by a company to its existing customers should be excluded from the prohibitions of proposed section 310.4(b)(1)(iii)(B). We also suggest that the Commission define an existing "customer" consistently with the definition of that term in the Commission's GLBA regulation (16 C.F.R. §313.3(h) and (i)) in order to provide clear guidance on who is and is not a "customer."

According to the Supplementary Information to the Proposal, the company-specific approach has been criticized by consumers and state law enforcement agencies as being unduly burdensome on consumers and ineffective in preventing unwanted telemarketing calls. The Commission cites instances in which consumers have had to make do-not-call requests repeatedly, as well as those in which consumers' do-not-call requests are ignored.

Unfortunately, we do not doubt that these practices occur. But, it is highly unlikely that this is happening where the business making the telemarketing call has an existing relationship with the consumer. When calling a consumer with which it has no existing relationship, a telemarketer that is not concerned with applicable law, much less the interests of consumers, could certainly take the position that it has nothing to lose by interfering with that consumer's right to be placed on its do-not-call list. To the extreme contrary, the company that is calling its own customer would have everything to lose with such behavior. This is because a company's customers and its reputation are its most valuable assets, without which it cannot survive in a competitive marketplace. A company risks losing both by failing to honor its customers' requests not to receive outbound telephone calls. Therefore, it acts contrary to its own interests in doing so. Additionally, from a cost perspective, a company has no interest in telemarketing those of its customers who have indicated their desire not to receive such calls. But, for those customers who do want to receive offers of special products and services, a company must be able to make such offers available by using the most cost efficient and convenient means. With no justifiable reason, the Proposal would severely restrict a company's ability to reach these customers. Certainly, the states that have adopted their own do-not-call list have seen the value in preserving the relationship between customer and business in this regard as all exempt from their do- not-call provisions telemarketing calls made to existing customers. Because of this inherent conflict between the Proposal and the states, a company that complies with all twenty state do-not-call laws would nevertheless be out of compliance with the Proposal. This is contrary to the concept of a simplified and centralized do-not-call list method. We, therefore, strongly urge the Commission to exclude outbound telephone calls made to existing customers from proposed section 310.4(b)(1)(iii)(B).

We also ask the Commission to re-examine its conclusion that the Proposal does not conflict with the TCPA. The Proposal does conflict with the TCPA with respect to telemarketing calls made to existing customers. While the TCPA allows a company to telemarket its own customers unless and until the customer directs it not to, the Proposal takes the exact opposite approach by prohibiting a company from telemarketing its own customers unless and until the company receives "express verifiable authorization" from the customer to do so. The TCPA, as well as the Rule, preserve the business relationship and properly leave it to the consumer and company to determine the course taken with respect the company's ability to make and the consumer's decision to receive offers for existing products and services over the telephone. On the other hand, the Proposal interferes with the business relationship between consumer and company and requires both to go through time consuming, costly, and burdensome steps in order to return the relationship to its intended state. Consequently, the consumer who places her name on the proposed do-not-call registry ("Registry") intending to prevent unwanted telemarketing

[1] See e.g., Alaska Stat. §45-50-475(g)(3)(B)(v); California Senate Bill 771 (2001), effective January 1, 2003; Colorado House Bill 1405 (2001), effective July 1, 2002; FL. Stat. Ann. 501.604(21); GA Code Ann. §46-5-27(b)(3)(B); ID Code §48-1002(12); LSA-R.S. §45:844.12(4)(c); Missouri Stat. Ann. §407.1095(3)(b); OR Rev. Stat. §646.569(2)(b); TN Code Ann. §65-5-401(6)(B)(iii).

calls from companies with which she has no relationship, but not intending to prevent telemarketing calls from the companies with which she does have a relationship, finds herself in the position of having to write or call (and, based on proposed section 310.4(b)(1)(iii)(B)(2), call only from the telephone number at which she will accept telemarketing calls) each and every company with whom she has a relationship in order to continue to receive offers for additional products and services by telephone. Likewise, the company with which the business relationship exists would have to establish and implement costly procedures in order to obtain and retain written or tape recorded evidence of all express verifiable authorizations received from its own customers. In this regard, many companies would also have to make significant capital expenditure in order to purchase equipment that enables them to determine the telephone number from which the consumer is calling and to tape record authorizations, as the Proposal would require. The imposition of these burdens will have the unfortunate effect of eliminating the telephone as the most cost efficient and convenient method available to companies in making offers of goods and services to their own customers. This loss of efficiency and convenience will lead to higher costs and fewer choices to the ultimate detriment of the consumer.

Outbound telephone calls made to former customers should also be exempted from proposed section 310.4(b)(1)(iii)(B) for some period of time after the customer relationship has ended. **A** number of states have adopted this approach. For example, in Louisiana[2], calls made to former customers are permissible where the customer relationship ended no more than six months prior to the call. In Colorado[3], this exemption is extended to calls made to former customers up to eighteen (18) months after the relationship ends. In both Texas[4] and Tennessee', a former customer can be contacted up to twelve (12) months after the relationship ends. And, some states allow calls to be made to former customers regardless of when the prior relationship ended.[6] Consequently, these and other state legislatures have recognized that even though an account that gives rise to an existing relationship may have been paid in full, it does not necessarily follow that the relationship between the company and the consumer is likewise terminated. Many consumers will choose one particular company as the provider of a product or service that they want or need from time to time. And, the approach taken by these and other states allows companies to continue to offer goods and services to the consumers they have served before to the benefit of both the consumer and the company. And, of course, should the consumer not wish to receive further offers, she can ask the company to discontinue calling. Therefore, we suggest that the Commission adopt the approach taken by these and other states by exempting from the restrictions of proposed section 310.4(b)(1)(iii)(B) calls made to former customers for at least twelve (1**2)** months after the existing customer relationship ends.

---

[2] LSA-R.S. §45:844.12(4)(c)
[3] House Bill 1405 (2001); July 1, 2002 effective date
[4] TX Bus. & Com. Code §43.003(b)(2)
[5] TN Code **Ann.** §65-4-401(6)(B)(iii)
[6] See e.g., FL Stat. **Ann.** §501.604(21); **GA** Code **Ann.** 46-5-27(b)(3)(B); OR Rev. Stat. §646.569(2)(b)

In conclusion, we believe the Commission's statement that the Proposal would provide consumers with a wider range of choices than does the original Rule, is flawed. Rather, the Proposal would have quite the opposite effect in terms of any existing business relationship by making it so difficult for both the consumer to exercise her choice and the company to honor it that any such choice is, in effect, forfeited once the consumer is on the Registry. For these and the foregoing reasons, the Commission should exclude outbound telephone calls made to existing customers, as well as former customers from proposed section 310.4(b)(1)(iii)(B). In addition, in order to preserve the synergies that the financial modernization provisions of the GLBA were designed to create, this exemption should extend to all members of a corporate family such that one company may contact a consumer if one of its sister companies has an existing or prior relationship with that consumer.

Proposed National Do-Not-Call Registry

As stated above, we believe that a centralized and simplified method to record and communicate a consumer's telemarketing preferences is a good approach in theory. While the Commission has taken a step in the right direction toward this end, our concern is that the Registry would simply be layered on top of an already complicated and inconsistent patchwork of existing state do-not-call lists. We commend the Commission for appreciating the importance of the economic burdens that compliance with a myriad of state do-not-call lists places on the industry. Clearly, these burdens will continue to grow as more and more states adopt their own do-not-call lists. Certainly a nationwide "one-stop shopping" approach is beneficial to both consumers and the industry. Therefore, if and when a Registry is established, it should either preempt or incorporate all state do-not-call lists such that, with either approach, a company's compliance with the Registry will constitute compliance with all state do-not-call lists.

Before the Registry can even be considered by consumers and the industry, however, there are a number of issues that must be addressed. First, how much will the Registry cost to establish and maintain, and how will it be funded? Who will have access to it and how will it be accessible? Will consumers have to pay a fee to be on the Registry? What will the cost be to access the Registry? The States are all over the board on this last question, with some lists available for as little as $10.00 and others costing as much as $800.00. We believe the cost for the Registry should not exceed $500.00 per year per corporate family (i.e., not per subsidiary), including updates. This suggested amount is based on an average of the amounts charged by the states and the Direct Marketing Association for their respective lists.

Another important item that must be more clearly addressed in the Proposal is what information will be on the Registry? As the Proposal currently reads, only a consumer's "name and/or telephone number" would be included. Does this mean the consumer would have the option of placing either her name or her telephone number on the Registry, but would not be required to include both? The industry is already dealing with inconsistent state requirements in this regard which increase the risk of error to the detriment of both consumers and businesses

alike. Some state do-not-call lists include the consumer's name and telephone number, some include the consumer's zip code and telephone number, and some only include the consumer's telephone number. Our concern is that the less information that is on a do-not-call list, the more chance for error, given the fact that so many consumers have the same name, and a single telephone number can belong or be transferred to more than one consumer. The more information that is on a do-not-call list, the more efficiently and accurately it can be used to honor the wishes of the consumers thereon. Consequently, at a minimum, the Registry should include the name, address, and telephone number of each consumer who chooses to be included thereon.

The Proposal provides that the Registry would be updated on a monthly basis. We believe this update schedule is too frequent and not workable given the fact that each monthly update would include information on consumers living in all 50 states and the District of Columbia. This would create a substantial burden on the industry that would find itself spending more and more time and resources continually updating its own do-not-call databases. A more cost effective and reasonable approach, and that which has been adopted by many of the states having do-not-call lists, is an annual list that is updated on a quarterly basis. This approach would also be less burdensome on the Commission.

The Commission correctly raises the question of what procedures should be in place with respect to updating the Registry when consumers change their telephone numbers or when area codes associated with those numbers change. Most states are silent in this regard, but we commend the Commission for recognizing that this issue is central to the establishment and delivery to the industry of an accurate Registry. Aside from impressing upon the Commission the importance of this issue, we would like to suggest that this situation is best addressed between the Commission, the local exchange carriers, and other telecommunications entities.

To answer the Commission's question of how long a consumer should remain on the Registry, we consulted U.S. Postal Service and U.S. Census Bureau data. According to the U.S. Postal Service, over 40 million Americans move every year. The U.S. Census Bureau reports that there were 284.7 million United States residents as of July 1,2001. Consequently, between 15% and 20% of consumers move each year. Therefore, we recommend that consumers remain on the Registry for no more than five or six years. At the expiration of that time period, those consumers who wish to remain on the Registry should be required to re-register and update any information that may have changed.

Another question posed by the Commission is whether third parties should be able to place a consumer's name on the Registry. We believe the answer to that question is no. Allowing third parties to opt consumers out of receiving outbound telephone calls will likely lead to inaccuracies and increase the potential for fraud and abuse. The Commission and the industry should not be put in the position of having to second guess the intentions of someone purportedly acting on behalf of a consumer in this regard. To protect the integrity **and** reliability of the

Registry, the only person who should be able to place the consumer's name on the Registry is the consumer. Any other approach is a disservice to the consumers and the industry who rely on the Registry.

We support the Commission's retention of the current calling time restrictions which represent a workable balance between the privacy of consumers and the regulatory burden on interstate commerce. Any approach that would allow consumers to pick the dates and times they can receive outbound telephone calls would simply be impossible to implement. Beyond the fact that this would completely overload any internal do-not-call database maintained by a company, consumers change their minds. The time and day that works for a consumer during one month, or even one week, may not work the following week or month based on a variety of ever changing facts and circumstances impacting their daily lives. While well-intentioned, we believe this approach is not cost effective, would complicate and frustrate the compliance efforts of the industry, and would ultimately provide no additional benefit to the consumer.

We believe the restriction imposed by section 310.4(b)(1)(iv) on selling, purchasing or using the Registry for any purpose other than compliance with proposed do-not-call provisions is adequate to protect consumers. Our concern, however, is that this section not be so broadly construed as to prohibit affiliated companies from sharing the same list for purposes of compliance. While some states having do-not-call lists allow affiliated companies to purchase and share one list, other states have required each affiliated company to purchase its own list. The ludicrous result of this requirement is that a family of companies must purchase the same list over and over again at significant cost to those companies without corresponding benefit to consumers. This is especially absurd when that family of companies utilizes a central do-not-call database for cost and efficiency purposes.

The other issue raised by proposed section 310.4(b)(1)(iv) is with respect to a company's use of the information contained on the Registry. In many instances the consumers on the Registry will already be customers of the company that obtained the Registry. So, that company already has in its possession the information on that list (e.g., name, address, and telephone number) and should not be restricted from using it for any other lawful purposes. Similarly, a company may also have information with respect to consumers on the Registry who are not yet customers, but are potential customers. Again, companies should not be restricted from using this information for other lawful purposes merely because it is also contained on the Registry.

Express Verifiable Authorization

The Commission asks whether the Proposal provides adequate guidance with respect to what information is sufficient to evidence a consumer's "express verifiable authorization" to receive outbound telephone calls from a particular company. We believe that proposed section 310.4(b)(1)(iii)(B) provides more than just guidance stating that such authorization is deemed verifiable if "either of the following means are employed". Thus, the Commission has set forth

two choices that a company must use to establish express verifiable authorization, one for oral and the other for written authorization. Since the burden will be on the company to establish that it has received express verifiable authorization to place an outbound telephone call to a consumer on the Registry, we would suggest that the company should have the flexibility to determine what constitutes such authorization. As discussed previously, each of the choices set forth in the Proposal raise considerable burdens for both consumers and businesses. And what will work for one company will not necessarily work for another. **A** more workable approach would be for the Commission to provide a non-exclusive list of examples that would constitute express verifiable authorization. The ultimate decision of whether to use one of the examples provided, or to develop another method based on the guidance those examples provide, should be left to the individual company as it is in the best position to know its capabilities in this regard.

Safe Harbor

We generally support the safe harbor provisions in section 310.4(b)(2). We agree with and commend the Commission's determination that strict liability is inappropriate where a company has made a good faith effort to comply with applicable do-not-call laws and a call that would otherwise violate section 310.4(b)(1)(iii)(B) is the result of bona fide error. For the reasons discussed above, however, the provision requiring companies to obtain and reconcile the Registry on not less than a monthly basis in order to take advantage of this safe harbor should be changed to instead require a quarterly update. In addition, a company's ability to timely reconcile an updated list depends on the format it is in and when it is made available. In order to give companies a reasonable opportunity to ensure that their own internal databases can be updated accurately, the safe harbor provisions should provide that an outbound call to a consumer on the Registry is not a violation of proposed section 310.4(b)(1)(iii)(B) if it is made no more than thirty (30) days after the most recent updated Registry becomes available. Many states have also adopted this approach.[7] **A** company should also be entitled to the safe harbor provisions to the extent any of the information contained in the most recent version of the Registry becomes inaccurate, such as a consumer's change of name or telephone number.

Finally, we are concerned with the proposed changes to section 310.4(b)(2)(ii) which would require a company to train its employees and "any entity assisting in its compliance". This change would appear to require a company to provide compliance training with respect to the Rule to any telemarketing vendor it engages. If this is the intention of the Commission, we strongly urge it to reconsider. Companies that engage telemarketing vendors to perform services on their behalf do so primarily for efficiency and cost savings purposes. To require the company to train the telemarketer in the first instance negates any savings that could have been realized. In addition, because vendors perform services for a multitude of companies, they could not continue to operate if required to change their procedures every time they perform services for a different company. The telemarketing vendor is relied upon by the company that hires it as an

[7] See e.g., NY Gen. Bus. §399-z 3. (provides for 30 days); TX Bus. & Com. Code §43.102(a) (provides for 60 days).

expert in the field in which it operates. Before hiring any vendor, a company confirms that the vendor has policies and procedures in place, and properly trains its employees, to ensure compliance with all applicable laws. Rather than requiring a company to train its vendors, it should be sufficient that it engages in this due diligence review and enters into a contract with the vendor that provides the company with rights and remedies it can exercise in the event the vendor fails to comply with applicable law. Therefore, if the Commission's intention with this language is to require companies to provide compliance training to the vendors they engage, the language should be stricken. If the language is designed to serve some other purpose, we respectfully request the Commission to provide clarification consistent with these comments.

Blocking Caller ID (§ 310.4(a)(6))

Caller identification services provide consumers with an important mechanism to exercise their choice with respect to who is contacting them. We agree that blocking, circumventing, or altering transmission of the name and telephone number ("Caller ID information") of the calling party for caller identification purposes is an abusive telemarketing act or practice. While we support the Proposal in this regard, if it is adopted in the final Rule, we strongly urge the Commission to expressly clarify that the use of telephone equipment that is incapable of displaying the name and telephone number of the calling party does not constitute "blocking" of Caller ID information in violation of the final Rule.

The Commission correctly notes in the Supplementary Information to the Proposal that it is technologically impossible for many telemarketers to transmit Caller ID information because of the type of telephone system they use. Telemarketers use this type of equipment because of the cost efficiency it provides, and it would be beyond the scope and authority of the Act for the Commission to affirmatively require telemarketers to purchase and use only telephone equipment that is capable of transmitting Caller ID information. One of the questions the Commission poses is how telemarketers currently comply with the requirements of those states that have passed legislation "requiring the transmission of full caller identification information". 67 Fed. Reg. 4492,4538. While a number of states have enacted Caller ID legislation, these laws prohibit the use of devices and methods to intentionally block Caller ID information, but do not affirmatively require the transmission of Caller ID information. For example, in Illinois the law specifically provides that it is a violation to "impede[s] the function of any caller id *when the telephone solicitor's service or equipment is capable ofallowing the display of the solicitor's telephone number."*' (emphasis added).

[8] $815 ILCS 413/15(c). Also see FL Stat. Ann. §501.616(7) (". . . unlawful. . . to prevent transmission. . . when equipment or service used by the telephone solicitor is capable of creating and transmitting the telephone solicitor's name or telephone number."); Utah Code **Ann.** §13-25a-103(6) **("A** telephone solicitor may not withhold the display of. . . telephone number from a caller identification service . . . when the telephone solicitor's service or equipment is capable of allowing the display of the number."); K.S.A. 50-670(c) **("A** telephone solicitor shall not withhold the display of the telephone solicitor's telephone number . . . when the telephone solicitor's service or equipment is capable of allowing the display of such number.").

For the foregoing reasons, we urge the Commission to clarify that the Proposal does not affirmatively obligate telemarketers to purchase and use telephone equipment that is capable of transmitting Caller ID information and that use of technology that is not capable of transmitting Caller ID information is acceptable.

Predictive Dialers

The Commission seeks recommendations on alternative approaches to the use of predictive dialers. In response to comments it reports to have received from consumers expressing frustration over "dead air" calls, the Commission asks whether it should establish a maximum abandon rate when predictive dialers are used, limit the use of predictive dialers to only those telemarketers that use equipment capable of transmitting Caller ID information, or allow telemarketers to play a tape recorded message until a live telemarketer is available to speak to the consumer. 67 Fed. Reg. 4492,4539.

It is undisputed that the proper use of predictive dialers increases the efficiency with which products and services can be made available to consumers over the telephone. While it is true that the misuse of predictive dialers can lead to consumer frustration, any regulation of call abandonment rates must be carefully weighed against the potential loss of the cost efficiencies provided by predictive dialers. For example, while requiring a zero percent call abandonment rate would effectively render illegal the use of predictive dialers, a low abandonment rate may limit the impact on consumers while preserving the cost benefits predictive dialers provide to the industry. With this in mind, we believe the Commission should conduct further study into current industry practices to determine what would be an acceptable call abandonment rate.

We do not believe that the use of predictive dialers should be limited to only those telemarketers that use technology capable of displaying Caller ID information. Such a rule would unfairly penalize and disadvantage telemarketers that choose to purchase and use more cost effective telephone equipment. Further, any cost savings realized by being able to use a predictive dialer under such circumstances would be lost on the purchase and use of more expensive telephone technology.

Since it appears that the primary issue with "hang ups" and "dead air" calls is that consumers don't know who is calling and why they are being called, the most logical approach may be to allow telemarketers to play a recorded message until a live telemarketer is available to speak to the consumer. This approach strikes a balance between the interests of consumers who want to know who is calling and the interests of telemarketers that wish to use the most cost efficient method of reaching consumers. If the Commission adopts this approach, however, the industry will need guidance as to the interplay of the final Rule with the TCPA's conflicting provision prohibiting the initiation of a call using a "prerecorded voice". 47 C.F.R. § 64.1200(a)(2).

Conclusion

Once again, we appreciate the opportunity to comment on this Proposal. If you should have any questions on the information contained in this letter, please feel free to contact either me at (847) 564-6324, or Martha Pampel, Associate General Counsel, at (847) 564-7941.

Sincerely,

Julie A. Davenport'
Associate General Counsel

Attachments

FTC TSR Comment Letter

If You Become a Victim of Identity Theft

If you believe that someone has stolen your identity, you should:

- **Contact the fraud department** of each of the three major credit bureaus to report the identity theft and request that the credit bureaus place a fraud alert and a victim's statement in your file. The fraud alert puts creditors on notice that you have been the victim of fraud, and the victim's statement asks them not to open additional accounts without first contacting you.

  The following are the telephone numbers for the fraud departments of the three national credit bureaus:
  Trans Union: 1-800-680-7289;
  Equifax: 1-800-525-6285;
  Experian: **1-88**8-397-3742.

  You may request a free copy of your credit report. Credit bureaus must provide a free copy of your report, if you have reason to believe the report is inaccurate because of fraud and you submit a request in writing.

- **Review your report** to make sure no additional fraudulent accounts have been opened in your name, or unauthorized changes made to your existing accounts. **Also,** check the section of your report that lists "inquiries" and request that any inquiries from companies that opened the fraudulent accounts be removed.

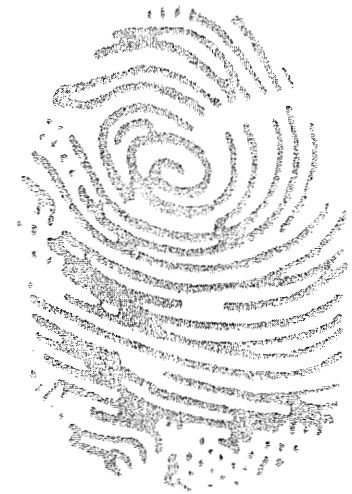
- **Contact any bank or other creditor where you have an account** that you think may be the subject of identity theft. Advise them of the identity theft. Request that they restrict access to your account, change your account password, or close your account, if there is evidence that your account has been the target of criminal activity. If your bank closes your account, ask them to issue you a new credit card, **ATM** card, debit card, or checks, as appropriate.

- **File a report with your local police department.**

- **Contact the FTC's Identity Theft Hotline toll-free at 1-877-ID-THEFT (438-4338).** The FTC puts the information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.

Comptroller of the Currency
Administrator of National Banks

How to Avoid Becoming a Victim of Identity Theft



What is Identity Theft?

Identity theft is the fraudulent use of a person's personal identifying information. Often, identity thieves will use another person's personal information, such as a social security number, mother's maiden name, date of birth, or account number to open fraudulent new credit card accounts, charge existing credit card accounts, write checks, open bank accounts, or obtain new loans. They may obtain this information by:

- Stealing wallets that contain personal identification information and credit cards.
- Stealing bank statements from the mail.
- Diverting mail from its intended recipients by submitting a change of address form.
- Rummaging through trash for personal data.
- Stealing personal identification information from workplace records.
- Intercepting or otherwise obtaining information transmitted electronically.

Pretext calling is a fraudulent means of obtaining a person's personal information. Pretext callers may contact bank employees, posing as customers, to access customers' personal account information. Information obtained from pretext calling may be sold to debt collection services, attorneys, and private investigators to use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information to create fraudulent accounts.

Here are a few basic steps you can take to avoid becoming a victim of identity theft and pretext calling:

- **Do not give personal information,** such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet, unless you initiated the contact or know with whom you are dealing.
- **Store personal information in a safe place** and tear up old credit card receipts, **ATM** receipts, old account statements, and unused credit card offers before throwing them away.
- **Protect your PINs and other passwords.** Avoid using easily available information, such as your mother's maiden name, your birth date, the last four digits of your social security number, your phone number, etc.
- **Carry only the minimum amount of identifying information** and number of credit cards that you need.
- **Pay attention to billing cycles and statements.** Inquire of the bank, **if** you do not receive a monthly bill. It may mean that the bill has been diverted by an identity thief.
- **Check account statements carefully** to ensure all charges, checks, or withdrawals were authorized.
- **Guard your mail from theft.** If you have the type of mailbox with a flag to signal that the box contains mail, do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail.
- **Order copies of your credit report** from each of the three major credit bureaus once a year to ensure that they are accurate. The law permits the credit bureaus to charge $8.50 for a copy of the report (unless you live in a state that requires the credit bureaus to provide you with one free copy of your report annually).
- **If you prefer not to receive preapproved offers of credit,** you can opt out of such offers by calling (888) 5 OPT OUT.
- **If you want to remove your name from many national direct mail lists,** send your name and address to:
  DMA Mail Preference Service
  P.O. **Box** 9008
  Farmingdale, NY 11735-9008
- **If you want to reduce the number of telephone solicitations** from many national marketers, send your name, address, and telephone number to:
  DMA Telephone Preference Service
  P.O. **Box** 9014
  Farmingdale, NY 11735-9014

OCC ADVISORY LETTER

Comptroller of the Currency
Administrator of National Banks

Subject: Identity Theft and Pretext Calling

TO: Chief Executive Officers of All National Banks, Department and Division Heads, and All Examining Personnel

I. PURPOSE

This advisory letter informs national banks about two areas of consumer bank fraud—identity theft and pretext calling—and advises them about measures to prevent and detect these types of fraud. The Gramm–Leach–Bliley Act (GLBA), enacted in 1999, directs the federal banking agencies (the Agencies) to ensure that banks have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information.[1] The Agencies recently adopted guidelines for the safeguarding of customer information by financial institutions.[2] The advisory letter supplements those guidelines by focusing on the protection of customer infomation specifically against identity theft and pretext calling.

Identity theft is the fraudulent use of an individual's personal identifying information. Often, identity thieves will use another individual's personal information such as a social security number, mother's maiden name, date of birth, or account number to fraudulently open new credit card accounts, charge existing credit card accounts, write checks, open bank accounts or obtain new loans. They may obtain this information through a number of means, including

- Stealing wallets that contain personal identification information and credit cards,
- Stealing financial institution statements from the mail,
- Diverting mail from its intended recipients by submitting a change of address form,
- Rummaging through trash for personal data,

[1] 15 USC 6825. GLBA also contains specific prohibitions against obtaining customer information from a financial institution by false pretenses. *Id.* at 6821.

[2] See Interagency Guidelines for Establishing Standards for Safeguarding Customer Information, 66 *Fed. Reg.* 8616 (February 1, 2001). The OCC's standards are codified at 12 CFR Part 30, App. B (hereinafter, referred to as the "Guidelines for Safeguarding Customer Information").

- Stealing personal identification information from workplace records, or

- Intercepting or otherwise obtaining information transmitted electronically.

Pretext calling is a fraudulent means of obtaining an individual's personal information. Pretext callers may contact financial institution employees, posing as their customers, in order to access customers' personal account information. Information obtained from pretext calling may be sold to debt collection services, attorneys, and private investigators for use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information for use in creating fraudulent accounts.

This advisory letter provides background information on identity theft and pretext calling and informs banks about: (1) relevant federal laws; (2) measures to take to reduce their risk of loss and protect their customers against these types of fraud; (3) how to report to law enforcement known or suspected federal criminal violations related to these types of fraud; and (4) the importance of consumer education to prevent fraud and assist individuals who have been victims of pretext calling and identity theft.[3]

11. BACKGROUND

According to the Federal Bureau of Investigation, identity theft is one of the fastest growing white-collar crimes in the nation.[4] More than 500,000 consumers are victimized each year by identity theft. This growing crime has a devastating effect on financial institution customers and a detrimental impact on the banks.[5] Four of the top five consumer complaints regarding identity theft involve financial services—new credit card accounts opened, existing credit card accounts used, new deposit accounts opened, and newly obtained loans.[6] Banks absorb much of the

[3] At the end of the advisory letter is an appendix that lists other OCC guidance regarding information security.

[4] Reasons cited for this increase in identity theft include the increased availability of personal information in the marketplace, the ability of identity thieves to use this information to, for instance, apply for credit under cover of anonymity afforded by remote channels, and the nearly instantaneous and ready availability of credit. ***See, e.g.,*** Testimony of the United States Secret Service to the House Committee on Banking and Financial Services, September 13,2000.

[5] For example, the American Bankers Association (ABA) 1998 Check Fraud Survey found that $3 out of every $4 lost by a community bank to check fraud was due to some form of identity theft. In its 2000 Check Fraud Survey, the ABA found that ***attempted*** check fraud doubled in the past two years, exceeding $2.2 billion dollars. The survey further indicated that one-third of fraud cases and fraud losses were due to forgery.

[6] On November 1, 1999, the Federal Trade Commission (FTC) established a toll-free telephone hotline, 1-877-ID-THEFT(438-4338), for consumers to report identity theft and seek counseling. Information from complainants is stored in a central database and used as an aid in law enforcement and prevention. In testimony delivered on September 13,2000, at a hearing on identity theft held by the House of Representatives Committee on Banking and Financial Services, the FTC reported that its identity theft hotline received over 1000 calls a week in July and August 2000. More recent public statements by FTC officials indicate that the number of calls to the hotline have more than doubled since then, to over 2000 calls a week. ***See, e.g.,*** Statement of Jodie Bernstein, director of the FTC's Bureau of Consumer Protection, to the President's Information Technology Advisory

economic losses from bank fraud associated with the theft of their customers' identities. Individuals who become victims of identity theft also pay, at a minimum, out-of-pocket expenses to clear their names and may spend numerous hours trying to rectify their credit records.[7]

Identity theft may go undetected for months and even years. Victims of identity theft may not realize that someone has stolen their identity until they are denied credit or until a creditor attempts to collect an unpaid bill.

Pretext calling is also difficult to detect. While information brokers and private investigators routinely advertise on the Internet and elsewhere their ability to locate and provide specific information about individual bank accounts, banks and their customers are likely to be unaware that they have been the victims of pretexting (*i.e.,* the use of some form of pretext to obtain customer information). Unless the pretexting ultimately leads to identity theft, it may go undetected altogether.

III. SUMMARY OF RELEVANT FEDERAL LAWS

Identity theft—In 1998, Congress passed the Identity Theft and Assumption Deterrence Act (18 USC 1028) (the Act). The Act makes it a crime to knowingly use, without lawful authority, a means of identification of another person with the intent to commit a crime, among other things. The unauthorized use of another individual's name, social security number, or date of birth to apply for a credit card is punishable by fine or imprisonment under this Act. The Act also requires the Federal Trade Commission (FTC) to establish a central complaint system to receive

---

Committee, February 7,2001. Information in the FTC database collected from hotline calls for the year 2000 indicate the most common forms of identity theft reported to the FTC include:

- Credit *card fraud*—Fifty percent of complainants reported that a credit card account had been opened in their name, or an identity thief had taken over their existing account. Seventy-one percent of these complaints involved the establishment of a new account; twenty-five percent involved the takeover of an existing account. (Roughly four-and-a-half percent of complaints in this category were unspecified.)

- Checking ***or*** savings *account fraud*—Sixteen percent of complainants reported a savings or checking account had been opened in their name or fraudulent checks had been written on existing accounts. Forty-nine percent of these complaints involved using unauthorized checks; twenty-seven percent involved establishing new checking accounts; seventeen percent involved unauthorized electronic fund transfers. (About seven percent of the complaints in this category were unspecified).

- Loanfiaud—Nine-and-a-half percent of complainants reported the identity thief had obtained a loan in their name.

See FTC Web site at www.consumer.gov/idtheft/. Click on FTC workshop and then on report charts.

[7] For example, under Regulation Z, in instances involving identity theft, a consumer could incur liability for the unauthorized use of the consumer's credit card account up to $50. Under Regulation E, a consumer's liability for unauthorized electronic fund transfers involving his or her account varies depending upon the precise circumstances of the unauthorized use and the consumer's timeliness in reporting unauthorized transactions or the loss or theft of an access card, number, or other device.

and refer identity theft complaints to appropriate entities, including law enforcement agencies and national credit bureaus.

Schemes to commit identity theft may also involve violations of other federal statutes such as the prohibition against fraudulent tax refund claims (18 USC 287), credit card fraud (18 USC 1029), computer fraud (18 USC 1030), mail fraud (18 USC 1341), wire fraud (18 USC 1343), or bank fraud (18 USC 1344). A number of states also have passed laws related to identity theft.

Pretext calling — The GLBA prohibits the making of false or fraudulent statements or representations to an officer, employee, or agent of a financial institution, or to a customer of a financial institution, to obtain customer information (15 USC 6821). The GLBA also prohibits anyone from requesting a person to obtain customer information of a financial institution, knowing that the person will use fraudulent methods to obtain information from the institution. Section 523 of the GLBA (15 USC 6823) imposes criminal penalties for knowing and intentional violations of these provisions.

While this statute is generally aimed at persons who victimize banks and their customers by attempting to obtain customer information through pretexting, banks could themselves be in violation of this statute if they use the services of any person who obtains customer information in violation of the statute. Although the statute maintains that an institution must "know" that the person will use artifice to obtain customer information, safe and sound banking practices dictate that a bank exercise reasonable diligence in selecting a third party to gather customer information. In this regard, banks should familiarize themselves with the methods used by third parties to collect customer information on their behalf. Banks should not the use the services of anyone the bank suspects may be engaging in pretexting to obtain customer information.

Security standards — Section 501(b) of the GLBA (15 USC 6801(b)) requires the Agencies to establish appropriate standards for banks relating to the administrative, technical, and physical safeguards of customer information. Banks are expected to take appropriate measures in accordance with the Guidelines for Safeguarding Customer Information to protect customer information against identity theft and pretext calling.

IV. MEASURES TO PREVENT IDENTITY THEFT AND PRETEXT CALLING

A. Identity theft

Identity thieves use a number of methods to obtain financial services in the name of another individual. For instance, an identity thief may request that a bank change the address on an existing credit card account, thereby diverting billing statements from the true account holder. Alternatively, an identity thief may order new checks on an existing account and have them sent to a mail drop, rather than the true account holder's address. An identity thief may use the personal information of another individual to apply for a new checking or credit card account.

Banks should employ a variety of methods to safeguard customer information and reduce the risk of loss from identity theft, including (1) verifying personal information to establish the identity

of individuals applying for financial products, (2) establishing adequate procedures to detect possible fraud in new accounts, **(3)** verifying the legitimacy of change of address requests on existing accounts, and (4) maintaining adequate security standards.

1. Verification procedures for new accounts

To reduce the risk of fraudulent applications, banks should establish verification procedures to ensure the accuracy and veracity of application information. In conjunction with their existing account opening procedures, banks should consider how best to independently verify information provided on account applications to detect incidents of identity theft. Verification of personal information may be accomplished in a number of ways. Some alternatives to consider include: (a) *positive verzfication* to ensure material information provided by an applicant is accurate; (b) *logical verification;* and (c) *negative verification* to ensure information provided has not previously been associated with fraudulent activity.*

a. Positive verzfication entails consulting third-party sources to assess the veracity of information submitted by a consumer. For example, an identity thief may provide the true name of an individual and a correct phone number, but an erroneous address. An institution could detect this discrepancy simply by checking a telephone directory. Under appropriate circumstances, a bank may obtain an individual's consumer report that would permit more detailed verification. Banks should consider calling a customer to confirm that the individual has opened a credit card or checking account, using a telephone number that has been verified independently. A phone call to a customer may alert an individual that his or her identity has been stolen. Additionally, a bank could contact an applicant's employer. **An** identity thief may provide the name of a legitimate employer, but may not provide the correct telephone number. A bank should attempt to contact an employer using an independently verified telephone number. Contacting an employer may expose a fraudulent application.

b. *Logical verification* entails assessing the consistency of infomation presented in an application. Such steps may reveal inconsistencies in the information provided by an applicant. For instance, a bank could verify if the zip code and telephone area code provided on the application cover the same geographical area. Products currently available from service providers can assist banks in verifying logical zip and area codes.

c. *Negative verzfication* entails ensuring that information provided on an application has not previously been associated with fraudulent activity.

2. Other new account procedures

Consumer reports can be an important source for preventing fraud. When processing **an** application for a new account, a bank may rely on a consumer report from a consumer reporting

[8] Some databases used for verification purposes may be provided by consumer reporting agencies and their use may raise issues under the Fair Credit Reporting Act.

agency. **A** consumer report of a victim of identity theft may be issued with a fraud alert.' When a bank has an automated system for credit approval, these systems should be designed to identify fraud alerts. Banks should not process an application when there is an existing fraud alert without contacting the individual in accordance with instructions that usually accompany a fraud alert *(i.e.,* a victim's statement), or otherwise employing additional steps to verify the individual's identity. The bank should have procedures in place to share a fraud alert across its various lines of business.

Consumer reports also may be a source for detecting fraud. Signs of possible fraudulent activity that may appear on consumer reports include late payments on a consumer's accounts in the absence of a previous history of late payments, numerous credit inquiries in a short period of time, higher-than-usual monthly credit balances, and a recent change of address in conjunction with other signs.

Finally, when an applicant fails to provide all requested information on an application, a bank should not process the incomplete application without further explanation.

3. Verifying change of address requests

A change of address request on an existing account may be a sign of fraudulent activity. A bank should verify the customer information before executing an address change and send a confirmation of the address change to both the new address and the address of record. If an institution gets a request for a new credit card or new checks in conjunction with a change of address notification, the bank should verify the request with the customer within a reasonable period of time after receiving the request.

4. Security standards

The Guidelines for Safeguarding Customer Information require banks to implement a comprehensive information security program that includes appropriate administrative, technical, and physical safeguards for customer information. Information security programs must be designed to ensure the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

Banks should take steps to secure the transmission and storage of electronic information to prevent identity thieves from gaining access to such information. This may include the use of encryption, firewalls, and other electronic data security systems and preventative measures. Identity thieves may also seek access to information that an institution discards. For instance, identity thieves may rummage through trash to collect customer information (dumpster diving). A bank should implement appropriate measures to restrict access to its customer records, such as

[9] **A** fraud alert is a statement that accompanies an individual's consumer report informing creditors that an individual's account has been the subject of fraud. Each of the major credit bureaus will voluntarily place a fraud alert on a consumer report upon request.

by shredding documents, to protect against dumpster diving and other forms of unauthorized access.

Banks and their service providers should implement appropriate controls and procedures to limit access to customer records. Because insiders may be identity thieves a bank should consider conducting background checks for its employees, in accordance with applicable law. Where indicated by its risk assessment, a bank should also monitor its service providers to confirm that they have implemented appropriate measures to limit access to customer records.[10]

B. Pretext calling

Pretext callers use pieces of personal information to impersonate an account holder in order to gain access to that individual's account information. Armed with personal information, such as an individual's name, address, and social security number, a pretext caller may try to convince a bank's employee to provide confidential account information. While it may be difficult to spot, there are measures banks can take to reduce the incidence of pretext calling, such as limiting the circumstances under which customer information may be disclosed by telephone.[11]

The Guidelines for Safeguarding Customer Information require banks to establish written policies and procedures to control risks to customer information, and consider access controls on customer information as part of these policies and procedures. Banks should take appropriate precautions against the disclosure of customer information to unauthorized individuals such as (1) limiting the circumstances under which employees may disclose customer information over the telephone, *(2)* training employees to recognize and report fraudulent attempts to obtain customer information, and (3) testing to determine the effectiveness of controls designed to thwart pretext callers.

1. Limiting telephone disclosures

There are a number of ways in which banks may limit access to customer information. One way is to permit employees to release information over the telephone only if the individual requesting the information provides a proper authorization code.[12] The code should be different than other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan, or other financial account numbers, or the maiden name of the customer's mother. The authorization code should be unique to, and capable of being changed readily by, the authorized

[10] For additional information on managing relationships with third-party service providers, ***see*** FFIEC guidance on technology outsourcing, "Risk Management of Outsourced Technology Services," (November 28, 2000).

[11] A bank should consider appropriate procedures and limits for disclosing information through any communication channel (*e.g.,* e-mail or wireless devices) that the institution uses. As the use and acceptance of e-mail, Internet banking, and electronic account statements increase, banks should develop procedures to verify the identity of the sender of a message. In many cases e-mail may not be an appropriate channel to communicate certain types of account information. E-mail can be easily forged, hijacked, or read by people other than the intended recipient. Additionally, a forger may be difficult to trace particularly if the message is relayed through intermediate mail servers.

[12] ***See, e.g.,*** OCC Advisory Letter 98-11 (August **20,** 1998).

account holder. To be most effective, the authorization code should be used in conjunction with other customer and account identifiers.

Another means of preventing unauthorized disclosures of customer information is to use a caller identification system (*i.e.*, CallerID™). If the telephone number displayed differs from that in the customer's account records, it may be an indication that the request is not legitimate and the employee should not disclose the requested account information without taking additional steps to verify that the true customer is making the request. In the absence of a caller identification system, banks could require employees who receive calls for account information to ask the caller for the number from which he or she is calling, or for a call-back number. If the individual refuses to provide the number, or it doesn't match the information in the customer's records, the employee should not disclose the information without additional measures to verify that the caller is the true customer.[13]

2. Employee training

Banks should train staff to recognize unauthorized or fraudulent attempts to obtain customer information. In addition to an employee's inability to match a caller's telephone number with that on file, there may be other indicators of a pretext call. For instance, a caller who cannot provide all relevant information requested, or a caller who is abusive, or who tries to distract the employee, may be a pretext caller. Employees should be trained to recognize such devices and, under such circumstances, protect customer information through appropriate measures, such as by taking additional steps to verify that the caller is a bona fide customer.

Employees should be trained to implement the bank's written policies and procedures governing the disclosure of customer information, and should be informed not to deviate from them. Moreover, employees must know to whom and how to report suspicious activity that may be a pretext call. Banks may have a fraud department or contact to whom the employee reports suspicious activities, or may establish another means for reporting possible fraud. Known or suspected federal criminal violations should be reported to law enforcement in accordance with the procedures discussed below.

3. Testing

Banks should test the key controls and procedures of their information security systems and consider using independent staff or third parties to conduct unscheduled pretext phone calls to various departments to evaluate the institution's susceptibility to unauthorized disclosures of customer information. Any weaknesses should be addressed through enhanced training, procedures, or controls, or a combination of these elements.

---

[13] There may be other circumstances in which a caller is seeking access to customer account information, such as a merchant attempting to verify whether the bank's customer has sufficient funds to cover a check. Banks should not permit their employees to provide a customer's account information without taking steps to verify the identity of the caller. For instance, banks could direct their employees to request a call back number to verify the merchant's identity. Additionally, where a bank uses an automated telephone response system to verify funds availability, the system should be password protected.

V. REPORTING SUSPECTED IDENTITY THEFT AND PRETEXT CALLING

OCC regulations currently require banks to report all known or suspected criminal violations to law enforcement and the OCC by the use of the Suspicious Activity Report *("SAR")*.

Criminal activity related to identity theft or pretext calling has historically manifested itself as credit or debit card fraud, loan or mortgage fraud, or false statements to the bank, among other things. Presumably, banks have been reporting such known or suspected criminal violations through the use of the SARs, in accordance with existing regulations.

As a means of better identifying and tracking known or suspected criminal violations related to identity theft and pretext calling, a bank should, in addition to reporting the underlying fraud (such as credit card or loan fraud) on a ***SAR***, also indicate within the ***SAR*** that such a known or suspected violation is the result of identity theft or pretext calling. Specifically, when identity theft or pretext calling is believed to be the underlying cause of the known or suspected criminal activity, banks should, consistent with the existing ***SAR*** instructions, complete a ***SAR*** in the following manner:

- In Part III, Box 35, of the ***SAR*** check all appropriate boxes that indicate the type of known or suspected violation being reported and, **in addition,** in the "Other" category, write in "identity theft" or "pretext calling," as appropriate.

- In Part V of the ***SAR***, in the space provided for the narrative explanation of what is being reported, include the grounds for suspecting identity theft or pretext calling in addition to the other violation being reported.

- In the event the only known or suspected criminal violation detected is the identity theft or pretext calling, then write in "identity theft" or "pretext calling," as appropriate, in the "Other" category in Part III, Box 35, and provide a description of the activity in **Part** V of the SAR.

Consistent with the ***SAR*** instructions, in situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, a bank should immediately notify, by telephone, the OCC and appropriate law enforcement, in addition to filing a timely suspicious activity report.

VI. CUSTOMER ASSISTANCE

Teaching prevention

Educating consumers about preventing identity theft and identifying potential pretext calls may help reduce their vulnerability to these fraudulent practices. Banks should consider making available to their customers brochures, newsletters, or notices posted in their lobbies or on their Web sites describing preventative measures consumers can take to avoid becoming victims of

these types of fraud. Banks are strongly encouraged to inform their customers of the following precautionary measures that law enforcement recommends to protect against identity theft and pretext calling:

Do not give personal information, such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet unless you initiated the contact or know with whom you are dealing.

Store personal information in a safe place and tear up old credit card receipts, ATM receipts, old account statements, and unused credit card offers before throwing them away.

Protect your PINs and other passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your social security number, your phone number, etc.

Carry only the minimum amount of identifying information and the number of credit cards that you need.

Pay attention to billing cycles and statements. Inquire of the bank if you do not receive a monthly bill; it may mean the bill has been diverted by an identity thief:

Check account statements carefully to ensure all charges, checks, or withdrawals were authorized.

Guard your mail from theft. If you have the type of mailbox with a Jag to signal the box contains mail, do not leave bill payment envelopes in your mailbox with the Jag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail.

Order copies of your credit report from each of the three major credit bureaus once a year to ensure they are accurate. The law permits the credit bureaus to charge $8.50 for a copy of the report (unless you live in a state that requires the credit bureaus to provide you with one free copy of your report annually).

If you prefer not to receive preapproved offers of credit, you can opt out of such offers by calling 1-888-5-OPT OUT.

If you want to remove your name from many national direct mail lists, send your name and address to:
DMA Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735-9008

If you want to reduce the number of telephone solicitations from many national marketers, send your name, address and telephone number to:
DMA Telephone Preference Service

P.O. Box ***9014***
Farmingdale, NY 11735-9014.

Assistance for Victims

There are a number of measures banks can take to assist victims of such fraud. These include:

(1) having trained personnel respond to customer calls regarding identity theft or pretext calling;

(2) determining if it is necessary to close an account immediately after a customer reports unauthorized use of that account, and issuing the customer a new credit card, ATM card, debit card or checks, as appropriate. Where a customer has multiple accounts with an institution, the institution should assess whether any other account has been the subject of potential fraud; and

(3) educating customers about appropriate steps to take if they have been victimized.
The following are measures banks may advise their customers to take if they are the victims of identity theft.

Contact the fraud departments of each of the three major credit bureaus to report the identity theft and request that the credit bureaus place a fraud alert and a victim's statement in your file. The fraud alert puts creditors on notice that you have been the victim of fraud and the victim's statement asks them not to open additional accounts without first contacting you. The following are the telephone numbers for the fraud departments of the three national credit bureaus: Trans Union: ***1-800-680-7289;*** *Equifax:* ***1-800-525-6285;*** *Experian:* ***1-888-397-3742.***

You may request a free copy of your credit report. Credit bureaus must provide a free copy of your report if you have reason to believe the report is inaccurate because of fraud and you submit a request in writing.

Review your report to make sure no additional fraudulent accounts have been opened in your name, ***or*** *unauthorized changes made to your existing accounts.* ***Also,*** *check the section of your report that lists "inquiries" and request that any inquiries from companies that opened the fraudulent accounts be removed.*

Contact any financial institution ***or*** *other creditor where you have an account that you think may be the subject of identity theft. Advise them of the identity theft. Request that they restrict access to your account, change your account password, or close your account if there is evidence your account has been the target of criminal activity.*

File a report with your local police department.

Contact the FTC's Identity Theft Hotline toll-free at ***1-877-ID-THEFT (438-4338).*** *The FTC puts the information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.*

The above measures are contained in a consumer brochure available on the OCC's Web site at www.occ.treas.gov/idtheft.pdf. Banks may download this information in the form of a trifold brochure and provide it to their customers.

Questions relating to this advisory should be directed to Amy Friend, assistant chief counsel, at (202) 874-5200.

_____

Nanette G. Goulet
Acting Deputy Comptroller
Community and Consumer Policy

APPENDIX: LIST OF OCC ISSUANCES REGARDING INFORMATION SECURITY

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 ***Fed. Reg.*** 8616,8632 (February 1, 2001), to be codified at 12 CFR Part 30, App. B
- OCC Alert 2000-09: Protecting Internet Addresses of National Banks (July 19, 2000)
- OCC Bulletin 2000-14: Infrastructure Threats—Intrusion Risks (May 15, 2000)
- OCC Alert 2000-01: Internet Security: Distributed Denial of Service Attacks (February 11, 2000)
- "Internet Banking" booklet in ***Comptroller's Handbook*** (October 1999)
- OCC Bulletin 99-9: Infrastructure Threats from Cyber-Terrorists (March 15, 2000)
- Check Fraud—A Guide to Avoiding Losses (February 2000)
- OCC Bulletin 98-38: Technology Risk Management: PC Banking (August 24, 1998)
- OCC Advisory Letter 98-11: Pretext Phone Calling (August 20, 1998)
- OCC Advisory Letter 91-4 : Use of Social Security Numbers for Automated Call Systems (July 24, 1991)
- OCC Banking Circular 229: Information Security (May 31, 1988)
- Banking Circular 226 : End-User Computing (January 25, 1988)