(15)

Evans, Sandra E

From: Daniel Bushell [daniel.bushell@etrade.com]
Sent: Monday, April 01, 2002 3:55 PM
To: 'study.comments@ots.treas.gov'
Subject: Comments on the GLBA Information Sharing Study

Importance: High

DOT Comments-ET Financial.doc

Below are comments from E*TRADE Financial regarding the solicitation for public comment for the Study on Information Sharing Practices Among Financial Institutions and Their Affiliates.

Dan Bushell
Business Manager, Government Affairs & Privacy
E*TRADE Group, Inc.
4500 Bohannon Dr.
Menlo Park, CA 94025

phone: 650.331.5472 fax: 650.331.6801
email: daniel.bushell@etrade.com

This e-mail is the property of E*TRADE Group, Inc. It is intended only for
the person or entity to which it is addressed and may contain information
that is privileged, confidential, or otherwise protected from disclosure.
Distribution or copying of this e-mail or the information contained herein
by anyone other than the intended recipient is prohibited. If you have
received this e-mail in error, please immediately notify the sender by
e-mail at daniel.bushell@etrade.com and telephone at 650.331.5472. Please
delete and destroy any copies of this e-mail.

<<DOT Comments-ET Financial.doc>>

1.a. Financial institutions share the following types of information with
affiliates: contact information (name, address, phone number, and email
address), other personally-identifiable information (date of birth, social
security number, account number, drivers license number), experiential and
transactional information (such as account balance and trading activity),
and certain other information (investment experience, asset level, net
worth, etc.).

1.b. Financial institutions share similar types of information with
nonaffiliated third parties: contact information (name, address, phone
number, and email address), other personally identifiable information
(typically social security number and account number), and certain
experiential and transactional information (such as account balance and
trading activity).

1.c. Yes, financial institutions (FI's) may share different types of information with affiliates than with nonaffiliated third parties (NTP's), specifically certain experiential and transactional information (type of transaction, credit history) which are not required to fulfill a service by the NTP, and certain other information (investment experience, asset level, net worth, etc.). However, some FI's may share additional types of information with NTP's that are acting on their behalf to fulfill a service (e.g., market research, providing additional financial services not provided by the FI, etc.).

1.d. FI's share information with affiliates to provide financial services that their customers seek, to offer them with a broader range of financial services, to improve their business experience with the FI, and to serve them more efficiently. In addition, information is shared with affiliates to protect the security of customer information, to improve products and services (including more cost effective products and services), and to more (cost) effectively market their products to customers.

1.e. FI's share information with NTP's for essentially the same reasons as affiliates.

1.f. FI's may voluntarily place certain limits on the sharing of information. With their affiliates, FI's may limit the types of information shared based on the purpose of its use (e.g., contact information only for marketing campaign, asset level for modeling purposes to better understand the customer, etc.) as well as limit employee access to this information on a "need-to-know" basis." With nonaffiliated third parties, FI's may also limit the types of information necessary for a specific purpose and also limit third party access. Contractual agreements with nonaffiliated third-parties may also require limits of use and disclosure of customer information and require the return or destruction of this information when the relationship terminates.

1.g. N/A

1.h. N/A

2.a. FI's maintain administrative, technical, and physical safeguards that comply with federal standards to guard customers' information. Administrative safeguards include limiting access to customers' information to those employees who need to know that information to provide products or services (such as customer service personnel), conducting internal audits of FI's business practices and procedures in order to protect customers' personal information, and recommending to customers ways to maximize security online and to protect their information.

Technical safeguards include placing account information on secure portions of Web sites, enabling servers with Secure Sockets Layer (SSL)

technology to prevent unauthorized parties from viewing customers' nonpublic personal information that they give or access during a secure session, providing secure transmission protocols for transferring customer information outside a FI's network, employing digital certificate services to authenticate that customers are transacting with the actual Web site, as well as requiring customers to enter a unique user name and password each time they access their account information online.

Physical safeguards include providing on-site security 24/7 (including electronic access, fingerprint ID access, video surveillance, etc.), limiting physical access to areas with access to sensitive information to only those employees that require it, locating equipment and systems in areas with reinforced structures and protective systems (e.g., protection from earthquake, fire, tornado, etc.), and providing redundant/backup systems.

Protections that FI's impose on their third party service providers may include any or all of the aforementioned safeguards, but generally include commercially reasonable efforts. Contracts with third party service providers may also provide the right to conduct audits of their security and privacy practices.

2.b. The safeguards described above are generally required under existing law such as GLBA. Conducting internal audits of privacy and security practices follow The Interagency Guidelines Establishing Standards For Safeguarding Customer Information (12 CFR 30, Appendix B) in that they require assessment, management and control of risk, adjustment of the (bank's) security program, overseeing service provider arrangements, and reporting results/recommendations to the Board of Directors.

2.c. Existing statutory and regulatory requirements generally protect information adequately, although guidelines are preferred since they are flexible enough to: 1) accommodate different types of FI's that may have different security protection requirements, and 2) adjust for the evolution of security protection technologies.

2.d. N/A

3.a. There are limited potential privacy risks that a customer faces when a FI shares customer information with an affiliate. These risks may include providing incrementally increased access to a customer's information. If a FI has implemented proper security protections and ensures that certain requirements are met by the NTP, privacy risks may be limited to the same level as those of the FI alone.

3.b. There are limited potential privacy risks that a customer faces when a FI shares the customer's information with a NTP. These risks may include providing incrementally increased access to a customer's information. If a FI has implemented proper security protections, privacy risks may be limited to the same level as those of the FI alone.

3.c. There are limited potential privacy risks that a customer faces when
an affiliate FI shares information obtained from another affiliate with a
NTP. These risks may include providing incrementally increased access to a
customer's information. If an affiliate has implemented proper security
protections, privacy risks may be limited to the same level as those of the
FI alone.

4.a. FI's benefit from sharing information with affiliates in several
ways. These include providing financial services that customers seek (in
order to recognize revenue), offering customers a broader range of financial
services (to increase revenue), improving the customer experience (to
maintain revenue), and to serve customers more efficiently (to reduce
costs). In addition, information is shared with affiliates to protect the
security of customer information (to maintain revenue), to improve products
and services (to increase revenue and reduce costs), and to more effectively
market products to customers (to increase revenue and reduce costs).

4.b. FI's benefit from sharing information with NTP's in essentially the
same ways as with affiliates.

4.c. Affiliates benefit when obtaining information from a FI for
essentially the same ways as described in 4.a.

4.d. Affiliates benefit from sharing information that they obtained from
other affiliates with NTP's in essentially the same ways as described in
4.a.

4.e. There would be numerous effects on FI's and affiliates of further
limitations on the sharing of information. Costs would increase since
marketing would be less effective in that campaigns would not reach the
right customers, and less efficient in that more customers would be sent
marketing materials since campaigns would be less targeted. In addition,
smaller FI's may not be able to effectively compete with larger FI's, since
they rely to a greater extent on sharing information with NTP's to conduct
services that they may not be able to provide on their own. This would
increase their costs because they may have to bring these functions in-house
(build versus buy decision). In addition, further limitations on
information sharing may ultimately force the exit of small companies from
the market, creating new barriers to entry. Costs may also increase since
the ability to target and identify fraud may be reduced because information
could not be shared freely in order to conduct investigations. Revenues may
also decrease since many of these increased costs may have to be passed on
to the customer, who may choose to decrease their transaction frequency or
discontinue their relationship with a particular FI. In addition,

decreased
revenues from additional or new products would result from increased product
cycle times and throughput. Lastly, other business processes would be less
efficient; resulting in lost revenues and/or increased costs because
workarounds, databases and systems would have to be restructured to comply
with these further limitations.

5.a. Customers benefit from the sharing of their information by a FI with
affiliates in several ways. These benefits include: receiving financial
services that they seek (or conversely not receiving services that they
don't seek), receiving offers for a broader range of financial services that
may be of interest to them, improving their business experience with the FI,
and receiving offers and prices beneficial to them based on their
creditworthiness or asset levels (e.g., lower mortgage rates, higher CD
interest rates, reduced fees for frequent traders, etc.). In addition,
customers would enjoy increased security of their information (from fraud
and identity theft), improved products and services tailored to their needs,
while also receiving fewer unwanted (but more relevant) marketing
solicitations from FI's and their affiliates.

5.b. Customers benefit from the sharing of their information by a FI with
NTP's in essentially the same ways as with affiliates.

5.c. Customers benefit by affiliates sharing information obtained from
other affiliates with NTP's in essentially the same ways as mentioned in 5.a.

5.d. N/A

5.e. Further limitations on the sharing of such information would
predominately have negative effects on customers. The positive effects
would include customers having greater control of how their information is
used. The negative effects would include: having fewer financial service
alternatives, not receiving offers for a broader range of financial services
that may be of interest to them, encountering poor business experience with
the FI, and not receiving offers and prices beneficial to them based on
their creditworthiness or asset levels (e.g., higher mortgage rates, lower
CD interest rates, same fees or all traders, etc.). In addition, customers
could experience increased security risks from fraud and identity theft
(because information could not be shared freely in order to conduct
investigations), and products and services could not be tailored to their
needs. Customers would also receive more unwanted (and less relevant)
marketing solicitations from FI's and their affiliates. In addition,
further limitations on information sharing may ultimately force the exit of
small FI's from the market, creating new barriers to entry that decrease
competition and increase prices overall. In these instances, customers that
are disadvantaged or have fewer FI alternatives (e.g., inner city, rural)

may experience negative effects such as greater commuting distances to obtain and increased prices for financial services and products.

6.a. Existing privacy laws (e.g., GLBA and FCRA) adequately protect the
privacy of customers' information in that they require that notice of a FI's
privacy policy/practices be provided to customers detailing what information
about them is collected and disclosed, how that information is used and what
choices they have in directing the use of that information. FI's must comply with these policies/practices and are subject to examinations (and
appropriate remedies) by appropriate financial regulatory bodies (SEC, OTS,
etc.). These laws also provide guidelines for the FI's security provisions
to safeguard customers' privacy/personal information. Regulations, market
forces, and evolving security/privacy technology have driven FI's to comply
with these privacy laws, and in some cases, exceed their requirements.

6.b. New or revised statutory or regulatory protections that would be useful to protect customer privacy should include federal preemption of state privacy legislation. This would standardize privacy legislation across the 50 states and would make it easier for FI's to fully comply with
federal legislation to protect the privacy of customers' information. This
would result in reduced costs for FI's, and allow them to deploy resources
more effectively in compliance with federal privacy laws.

7.a. FI privacy notices have been adequate in light with existing requirements because they provide the pertinent information for customers to
make informed business decisions about their FI and how their information
can be used. The regulations also are adequate as to when, where, and how
notice and choice are provided so that a customer has the appropriate opportunity to make these decisions before entering a relationship with a
FI.

7.b. New or revised guidelines, not requirements, could improve how FI's
describe their privacy policies and practices, and inform customers about
their privacy rights. Specifically, the language required by GLBA (e.g.,
nonpublic personal information, opt-out, etc.) could be confusing to some
customers. Providing examples of industry "best practice" privacy notices
as an addendum to current regulations could be used as guidelines for future
privacy notices in order to alleviate possible customer confusion.

8.a. It is not feasible to require FI's to obtain customers' consent (opt-in) before sharing information with affiliates or NTP's in any circumstance because opt-ins destroy the potential synergies of sharing information for both FI's and consumers. The positive effects would include
obtaining a group of customers, albeit a small number, that would be

willing
to transact freely with the FI. Negative effects of opt-in would include
increased costs and decreased revenues since less information would be shared. Marketing would be less effective in that campaigns would not reach
the right customers, and less efficient in that more customers would be sent
marketing materials since campaigns would be less targeted. In addition,
smaller FI's may not be able to effectively compete with larger FI's, since
they rely to a greater extent on sharing information with NTP's to conduct
services that they may not be able to provide on their own. This would increase their costs because they may have to bring these functions in-house
(build versus buy decision). In addition, opt-in may ultimately force the
exit of small companies from the market, creating new barriers to entry. Also, costs may increase since the ability to target and identify fraud may
be reduced because information could not be shared freely in order to conduct investigations. Revenues may decrease since many of these increased
costs may have to be passed on to the customer, who may choose to decrease
their transaction frequency or discontinue their relationship with a particular FI. In addition, decreased revenues from additional or new products would result from increased product cycle times and throughput. Lastly, other business processes would be less efficient (resulting in lost
revenues and/or increased costs) because workarounds, databases and systems
would have to be restructured to comply with these further limitations.

For consumers, the positive effects would include having greater control of
how their information is used, but at the expense of several negative effects. These negative effects would include: having fewer financial service alternatives, not receiving offers for a broader range of financial
services that may be of interest to them, encountering a poor business experience with the FI, and not receiving offers and prices beneficial to
them based on their creditworthiness or asset levels (e.g., higher mortgage
rates, lower CD interest rates, same fees or all traders, etc.). In addition, customers could experience increased security risks from fraud and
identity theft (because information could not be shared freely in order to
conduct investigations), and products and services could not be tailored to
their needs. Customers would also receive more unwanted (and less relevant)
marketing solicitations from FI's and their affiliates. In addition, obtaining up-front consent for information sharing may ultimately force the
exit of small FI's from the market, creating new barriers to entry that decrease competition and increase prices overall. In these instances, customers that are disadvantaged or have fewer FI alternatives (e.g., inner
city, rural) may experience negative effects such as greater commuting distances to obtain and increased prices for financial services and products.

8.b. It would be appropriate to permit FI's to obtain customers' consent (opt-in) before sharing information with an affiliate as an alternative to a required opt-out at the sole discretion of the FI. An opt-in before sharing information with NTP's may be appropriate in limited circumstances where the NTP provides a non-financial product or service for customers that is promotional in nature (such as a retailer). Positive and negative effects for customers and FI's have been described previously (in 8.a.); however, allowing market forces and FI's to make the determination as to whether opt-in or opt-out is more appropriate is the best option.

8.c. It is not feasible to require FI's to permit customers to opt-out generally of having their information shared with affiliates because of reasons previously described in 4.e. and 5.a. It is not apparent to customers what the consequences would be for opting out of having their information shared with affiliates. However, if a FI has affiliates that provide products and services that are not financial in nature, permitting customers to opt-out generally of having their information shared with these affiliates may be feasible. The negative effects would be the same as mentioned previously, but there would be additional positive effects for customers in that not only would they be able to exercise greater control over their data, but they would not receive unwanted (i.e., non-financial) products and services. FI's may experience positive effects in this case, resulting in an enhanced business relationship since customers may perceive them as more trustworthy. This could help FI's in maintaining revenue from customers who might otherwise terminate their business relationship if they were upset at receiving non-financial products and services from the FI.

8.d. N/A

9.a. The circumstances which customers may be able to restrict the sharing of information by FI's for specific uses or direct the uses for which such information may be shared should conform to GLBA and FCRA (i.e., opt-out for NTP with the exception of service providers, joint marketing, etc.) and be at the discretion of the FI who provides those choices to the customer. Such circumstances may include opt-outs for sharing information with a non-financial services company that offer promotions to the FI's customers.

9.b. These circumstances have had some positive and negative effects for FI's and customers. FI's have to now incur additional costs to comply with the choice requirements of GLBA and FCRA, and devote additional resources to support the choice activities of its customers. However, this may create goodwill between the FI and its customers. Customers have experienced

some
negative effects regarding confusion as to the tradeoffs of opting-out from
sharing their information. However, for customers that do understand the
tradeoffs, the positive effects include exercising greater control over how
their information is used, and greater loyalty to their FI.

9.c. In accordance with GLBA, E*TRADE Financial provides an opt-out for
sharing customer information with Target, our partner retailer, where
customers can sign up for an account through E*TRADE Zones at select Super
Target stores or via a co-branded web site. After providing notice of our
privacy policy to our customers, some, who did not apply for an account
through these channels, chose to opt-out of having their information shared
(even though their information would not be shared with the retailer in this
instance). We devoted many resources to Customer Service for handling of
these customer inquiries and opt-out requests. As a result, we plan to
revise our privacy policy to better explain how information is shared with
our retail partners. Anecdotally, we have received few complaints since
resources were provided to Customer Service to address this issue,
signifying that our customers are satisfied with this practice.