Privacy Rules for Trust

Trust Management Network
June 19, 2019

Marilyn Smith
Consulting Principal
First Dimensions Consultants

Principles of the Privacy Rules

1. Disclose to your customers how their information is being used
2. Restrict unauthorize disclosure of confidential customer information

Principles of a Trust

1. Duty to Inform
2. Duty to Keep and Protect confidentiality of beneficiaries' information

Gramm-Leach- Bliley Act , 1999, amended 2015

Part 1

1. Notices to customers
2. Sharing restrictions
3. Opt-out opportunity

Part 2

1. Safeguarding Customer Information

Part 3

Required other federal agencies to adopt the rules implementing notice requirements and sharing restrictions and appropriate standards to protect customer information.

Other Agency Privacy Rules

- Regulation P
  - Initially adopted by Federal Reserve Board allowing alternative delivery methods including posting on website; rescinded in 2014 deferring to the CPFB's Reg P; amended by CFPB in 2018 removing notice requirements for consumers under certain circumstances, adopting 2015 GLBA amendments
- SEC Regulation S-P/ Privacy of Consumer Financial Information
  - Adopted By Securities & Exchange Commission for Registered Investment Advisors as Privacy of Consumer Financial Information
- Fair Credit Reporting Act

  Remained applicable under certain conditions prohibiting a financial institution from becoming a credit reporting agency,

Flip Side

- Right to Financial Privacy

  Provides procedure that the federal government must follow to request your customer records

Safeguarding Confidential Information Rules

Establish standards to protect customers information and records against threats or unauthorized access

- Data Security Act, 2015 / Interagency Guidelines

  Protect financial information relating to consumers, require notice of data security breaches, and comprehensive information security program

- Security Standards for Customer Information / Interagency Guidelines

  Implementing GLBA's Safeguarding Customer Information provisions

- Host of State laws directed at data security and breaches

Applicability to Trusts at a financial institution

For purposes of defining a ‘consumer”…

In the case of a Trust, the Trust is the customer, therefore neither the grantor or the beneficiary is consumer

In the case of an Employee Benefit Plan, the Plan is the customer, and is therefore not a consumer

In the case of a Fund holder, the holder is a customer of the Fund, and is not a consumer

However, a beneficiary or grantor may trigger the definition of a *consumer* when *applying* for financial services for *personal* reasons, even if the application is denied, triggering provisions of the Fair Credit Reporting Act and pt-out provisions if sharing. And fiduciaries still owe clients the duty of informed and confidentiality contained within privacy notices.

Notices

All customers must receive an initial and annual **privacy notice** disclosing your practices

- Initial Notice - at the time the relationship is established
- Annual - within a consistent 12-month period after the initial notice

  Annual means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply a consistent basis.
- Revisions - as to practices or details of the privacy notice, must send new privacy notice as soon as practical. May not wait until annual period.

Example

You provide a notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For example, if your initial notice was provided on any day of year 1, then you must provide an annual notice by December 31 of year 2. And by December 31 of each year following.

Model Privacy Forms of the regulations provide specifics for what must be included in the notices.

Gramm-Leach- Bliley Act 2015 amendment, effective 9/17/2018

Removed annual notice requirement to customers for financial institutions if:

- Financial institution does not share nonpublic personal information about customers, AND
- Financial institution has not changed it policies and procedures with regard to the disclosures

In other words

No revisions in sharing practices and no revisions in collection, information classification or types, or any part of what is stated on the most recent privacy notice sent. You cannot change practices to take advantage of the amendment.

Sharing / Disclosing

I. Sharing with
   a. Affiliate allowed, as stated on privacy notices you provide
   b. Non-affiliate prohibited, unless you provide customer or non-customer with an opportunity to opt-out

AND

II. If information to be shared is:

Personal , not publicly available

such as: name, address, phone number, income or

Mere fact that the individual has come to you and provided information seeking your service or product, even if relationship was not established

- If sharing, you must provide privacy notice and allow customer or non-customer to opt out.
- Preferences to opt-out remain effective until revoked by the customer or until the relationship terminates.
- Sharing of account numbers or account access numbers is prohibited.

Opt-out Opportunity

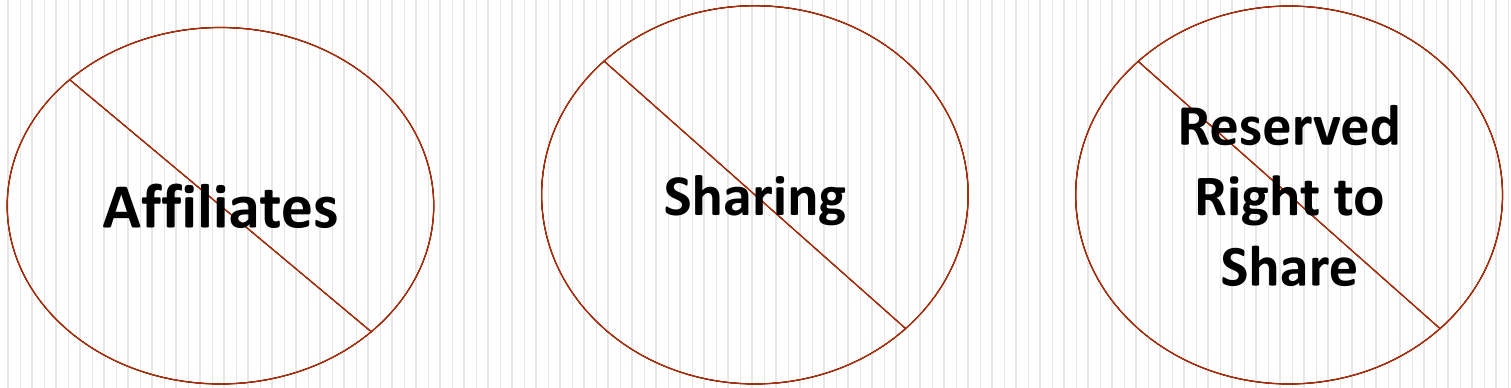
If you will share the **personal nonpublic** information that you have about a customer or a prospective customer [consumer] with a **nonaffiliated 3rd party**, you must provide that customer or consumer with an opportunity to opt-out of that sharing.

A customer or prospective customer is a *consumer* if they are seeking to obtain financial services or products from you for personal, family, or household purposes.

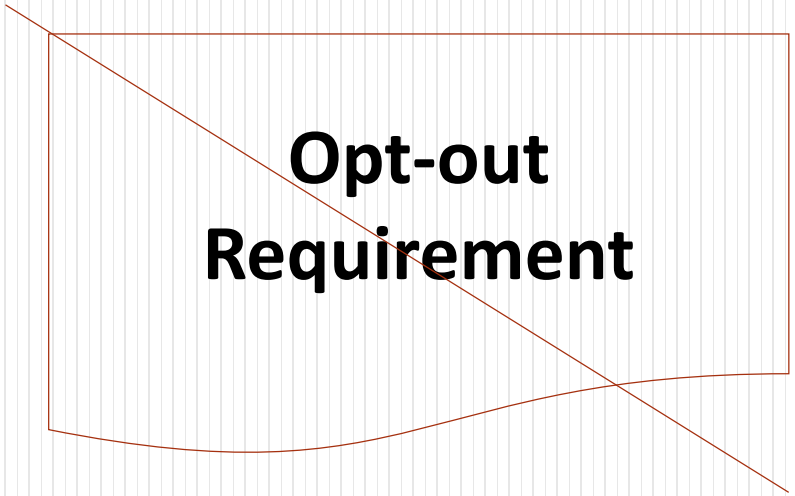
If seeking to obtain services or product for business purposes, the customer or prospective customer is not a consumer.

Opt-out Opportunity

IF



THEN



Opt-out Opportunity

- No affiliates, **and** no sharing except to servicers **AND** not reserving the right to share - then provide an initial and annual privacy notice only, no opt out

- Customers cannot opt out of 3rd party nonaffiliate sharing with service providers or as required to effectively administer or services

  However, the service should be under a written service agreement and the service provider would be subject re-disclosure limitations.

- If a customer opts out of all communications, there is also no privacy notice requirement; but you must make the privacy notice available upon request

Joint Accounts Opt-outs

May elect the Single or Separate practice of effecting opt out opportunities

- Single
  - Must accept direction from either
  - Treat opt out by either as opt out for entire account

- If allowed to opt-out separately
  - Must disclose this in your privacy notice
  - Accept opt out instructions from either for both/all parties
  - If 1 opts out, and other does not, you cannot share info of the one that opts out (cannot disclose fact that there is another party)

Joint Account Opt-outs

Single

A. You may send a single opt out notice to one address, but you must accept an opt out direction from either account holder;
B. You must treat an opt out direction by either account holder as applying to the entire account. If you do so, and one opts out, you may not require the other to opt out as well before implementing the one opt out direction; or
C. You must permit either account holder to opt out for each other.

Separate or Individual

A. You must permit either account holder to opt out for the other account holder;
B. If both opt out, you must permit both to notify you in a single response (such as on a form or through a telephone call, or website) and provide a reasonable amount of time for each to opt out
C. If one opts out and the other does not, you may only disclose nonpublic personal information about the one, but not the other, and cannot disclose existence of a joint relationship.

Safeguarding Customer Information

Each regulatory agency adopted rules to implement the safeguarding provisions and retained authorities to impose sanctions:

FRB, FFIEC, FDIC, NCUA, OCC, FTC- jointly sometimes referred as “Interagency”

As well a SEC and FINRA

Safeguards rules require:

- Designating at least one employee to manage the safeguards,
- Constructing a thorough [risk management] on each department handling the nonpublic information,
- Develop, monitor, and test a program to secure the information, and
- Change the safeguards as needed with the changes in how information is collected, stored, and used.

Breaches

Breaches are generally imposed under FIRREA ("Financial Institutions Reform, Recovery, and Enforcement Act").

In addition to reputational damage. Penalties under FIRREA may be up to :

- $9,468 per day
- $47,840 per day

  if found in violation or to have engaged in reckless unsafe or unsound practices or part of a misconduct pattern that results in minimal loss to bank and/or any financial gain to the parties involved
- $1,893,610 per day

  for knowingly committing a violation or causing substantial benefit any party involved

The SEC, FINRA and PCOAB may also impose separate sanctions for its members which may include criminal charges.

Additionally, States may impose restitution, fines, and penalties for data breaches.

On the horizon

Europe's GDPR – Global Data Protection Rules, passed 4/2016, eff 5/25/19

Basic principle is the fundamental right to data privacy or privacy by design

- Expands definition of personally identified information
- Disclose identity of data protection officer
- Contract detail regarding who has the data and why
- Recipients of data
- Sanctions up to £20Mil or 4% of annual revenues

States have begun seeking legislation to amend their breaching laws.

References

Guidance on How to Comply with the Privacy Rule of GLBA

https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

Regulation P FAQs: although Reg P was rescinded by the FRB in deference to the CFPB's authority, these offer a good set of FAQs.
https://www.federalreserve.gov/boarddocs/press/general/2001/200112122/attachment.pdf

Final Model Privacy Forms and GLBA
https://www.ftc.gov/sites/default/files/documents/federal_register_notices/final-model-privacy-form-under-gramm-leach-bliley-act-16-cfr-part-313/091201gramm-leach.pdf