INTRODUCTION
The privacy law was passed as part of the Gramm-Leach-Bliley (GLB) Act to modernize the banking laws, which was signed by the President on November 12, 1999 as Public Law 106-102.

The Financial Services Regulatory Relief Act of 2006 amended the GLB Act to require the federal regulatory agencies to propose a succinct and comprehensible model form that allows consumers to easily compare the privacy practices of different financial institutions and has an easy-to-read font. In November 2009, the agencies released a final model privacy notice form to be used by financial institutions to comply with the GLB Act.

Up until 2012, federally insured credit unions followed NCUA's privacy regulations, while state chartered, privately insured credit unions "officially" followed the privacy regulations issued by the Federal Trade Commission (FTC). With FTC's blessing, privately insured credit unions relied heavily on NCUA's rules as guidance because they addressed credit union specific issues. This all changed with the passage of the Consumer Financial Protection Act of 2010 (commonly referred to as the Dodd-Frank Act). The Dodd-Frank Act transferred all of the consumer privacy regulations (along with many other consumer protection regulations) to the, soon-to-be established, Consumer Financial Protection Bureau (CFPB).

Although there is now only one set of consumer privacy regulations for all credit unions, "credit union" is defined as "a Federal or state-chartered credit union that the National Credit Union Share Insurance Fund insures." This leaves state chartered, privately insured credit unions under the definition of "financial institution" and the jurisdiction of the Federal Trade Commission. (12 CFR §1016.3(l)(3). However, the provisions of the regulations that apply specifically to "financial institutions" rather than "credit unions", do not translate well for state chartered privately insured credit unions, so we have, for the most part, only included reference to the credit union provisions in this summary and recommend state chartered privately insured credit unions follow this guidance, as well.

WHAT CREDIT UNIONS GENERALLY MUST DO TO COMPLY

Overview: Generally, the privacy regulation is a disclosure rule and does not prohibit a credit union from sharing information with businesses outside of the credit union ("affiliates" and "nonaffiliated third parties"). However, you may not, directly or through any affiliate, disclose any nonpublic personal information about a member/consumer to a nonaffiliated third party unless:
(1) you have provided an initial notice to the member/consumer;
(2) you have provided an opt out notice to the member/consumer;
(3) you have given the member/consumer a reasonable opportunity to opt out before you disclose the information to nonaffiliated third parties, and
(4) the member/consumer does not opt out. [§1016.10(a)]

All credit unions have to provide privacy notices: All credit unions will be required to provide a privacy notice to people using their products and services even if a credit union does not share any information with a third party for marketing purposes.

"Opt out" option: Generally, before a credit union can share information with a nonaffiliated third party for marketing purposes, the credit union will have to give the person a reasonable opportunity to request that the information not be shared -- that is, the person has a right to "opt out" of the planned information sharing. However, this "opt-out" right does not exist when the credit union shares information with a third party to complete the requested transactions (such as sharing with a data processor) (§1016.14(a)), has a "joint agreement" (marketing contract) with a third party that is a financial institution (§1016.13), has the member's consent to share the information (§1016.15), or does so under another exception listed in the regulation. The credit union, however, can provide the opt-out option to anyone, if it chooses to do so. [§1016.7]

Model Privacy Form: Model privacy forms are included in the Appendix to the regulation. Although using the model forms is not mandatory, CUNA strongly encourages all credit unions to use the model forms because doing so constitutes compliance with the notice content requirements of the regulation. Although a member cannot sue your credit union under the privacy regulation, examiners and consumer groups may question why your credit union isn't using the model privacy form, which was developed to allow consumers to better understand privacy policies and compare the policies of different financial institutions.

Prohibition on sharing account numbers: The one prohibition in the law is that every credit union is forbidden from providing an account number or similar access number for a credit card account, share account or transaction account of any member to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing efforts. Exceptions: This prohibition does not apply if you disclose this information to: (1) your agent or service provider solely in order to perform marketing for your own products and services, as long as the agent or service provider is not authorized to directly initiate charges to the account, or (2) a participant in a private label credit card program or an affinity or similar program where the participants in the program are identified to the member when the member enters into the program.
Account number does not include: a number or code that is in an encrypted form, as long as you do not provide the recipient with a means to decode the number.

Transaction account does not include: an account to which third parties cannot initiate charges. [§1016.12]

INITIAL PRIVACY NOTICE

Your credit union must provide an initial privacy notice to any consumer who obtains a financial product or service from you that is to be used primarily for personal, family, or household purposes. For example:

- A member as defined in your bylaws;
- A nonmember who has a share, share draft, or credit card account with the credit union jointly with a member;
- A nonmember who has a loan that the credit union services;
- A nonmember who has an account with a credit union that has been designated as a low-income credit union; or
- A nonmember who has an account in a federally-insured, state chartered credit union pursuant to state law.

Delivery of the Initial Notice  [§1016.4(a)]

Members: The notice must be provided when they join the credit union, unless: (1) it would substantially delay the member’s transaction and the member agrees to receive the notice at a later time, or (2) you acquire a member’s deposit liability from another financial institution and the member does not have a choice about the acquisition. In these cases, it may be delivered within a reasonable time. [§1016.4(e)]

Nonmembers: The notice must be provided before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party.

Existing members: You must provide a revised privacy notice that covers the member’s new financial product or service, or if the most recent initial, revised, or annual notice provided to the member was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice. [§1016.4(d)]

ANNUAL PRIVACY NOTICE  [§1016.5]

The privacy rule initially required credit unions to send annual privacy notices to all members annually. This was an expensive and burdensome requirement. CUNA pushed hard for several years to have this requirement amended. When the regulatory agency’s attempts to address this burden were insufficient (an alternative delivery method), CUNA turned to Congress for relief from this regulatory burden. In December 2015, Congress passed the FAST Act, which included an amendment to the annual
privacy notice requirement. In 2018, the CFPB finally updated the regulation to limit the annual privacy notice requirement.

According to the regulation, credit unions must provide a clear and conspicuous notice to consumers that accurately reflects your privacy policies and practices not less than annually during the continuation of the member relationship. Annually 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 it to the member on a consistent basis.

**When An Annual Privacy Notice Is NOT Required**

You are not required to deliver an annual privacy notice if you:

(i) Provide nonpublic personal information to nonaffiliated third parties only in accordance with an exception listed in the privacy rule; and

(ii) Have not changed your privacy policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most recent privacy notice sent to the member.

**Former members/nonmembers:** You are not required to provide an annual notice to a former member/nonmember. An individual becomes a former member/nonmember of a credit union when:

(i) The individual is no longer the credit union's member as defined in the credit union's bylaws;

(ii) In the case of a nonmember's share or share draft account, the account is inactive under the credit union's policies;

(iii) In the case of a nonmember's closed-end loan, the loan is paid in full, the credit union charges off the loan, or the credit union sells the loan without retaining servicing rights;

(iv) In the case of a credit card relationship or other open-end credit relationship with a nonmember, the credit union no longer provides any statements or notices to the nonmember concerning that relationship, or the credit union sells the credit card receivables without retaining servicing rights; or

(v) The credit union has not communicated with the nonmember about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material.
DESIGN AND FORMAT OF YOUR PRIVACY NOTICES (includes Opt Out Notices)  
[§1016.3(b)]
Your privacy notices must be "clear and conspicuous", which means the notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

For example:
- Present the information in the notice in clear, concise sentences, paragraphs, and sections;
- Use short explanatory sentences or bullet lists whenever possible;
- Use definite, concrete, everyday words and active voice whenever possible;
- Avoid multiple negatives;
- Avoid legal and highly technical business terminology whenever possible;
- Avoid explanations that are imprecise and readily subject to different interpretations;
- Use a plain-language heading to call attention to the notice;
- Use a typeface and type size that are easy to read;
- Provide wide margins and ample line spacing;
- Use boldface or italics for key words; and
- When you combine your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars.

Website Notices: To call attention to the privacy notice on your website you should use text or visual cues to encourage scrolling down the page, if necessary, to view the entire notice. Additionally, make sure that other items on your website, such as text, graphics, hyperlinks or sounds do not distract attention away from your privacy notice.

Also, you must either:
- Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or
- Place a link on a screen that consumers frequently access that connects directly to the notice and is labeled appropriately to convey the importance and nature of the notice.

CONTENT OF THE PRIVACY NOTICE  
[§1016.6]
Using the Model Form meets the content requirements  
[§1016.6(f)]
See also Short-Form Initial Notice for nonmembers below  
[§1016.6(d)]
The initial, annual, and revised privacy notices must include each of the following items of information, in addition to any other information the credit union wishes to provide:
• **The categories of nonpublic personal information that you collect.** For example: information from the consumer, information about the consumer's transactions with you or your affiliates, information about the consumer's transactions with nonaffiliated third parties, and information from a consumer reporting agency.

• **The categories of nonpublic personal information that you disclose.** You can satisfy this requirement by listing the applicable categories you listed in the bullet above (information that you collect), with a few examples to illustrate the type of information in each category. However, if you reserve the right to disclose all of the nonpublic personal information that you collect from your members, you may simply state that fact, without describing the categories or using examples.

**Future disclosures:** Your notice may also include categories of nonpublic personal information that you reserve the right to disclose in the future, by do not currently disclose. [§1016.6(e)]

• **The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information.** Exception: When you disclose the information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes [§1016.14] or when one of the other exceptions apply. [§1016.15]. See EXCEPTIONS TO THE OPT OUT REQUIREMENTS later in this SUMMARY.

**Future disclosures:** Your notice may include categories of affiliates or nonaffiliated third parties to whom you reserve the right in the future to disclose but to whom you do not currently disclose, nonpublic personal information. [§1016.6(e)]

You satisfy disclosing these categories if you list the following, as applicable, and a few examples to illustrate the types:

- **Financial Service Providers.** Examples may include: mortgage bankers, securities broker-dealers, and insurance agents,
- **Non-financial Companies.** Examples may include: retailers, magazine publishers, airlines, and direct marketers; and
- **Others.** Examples may include: nonprofit organizations.

• **The categories of nonpublic personal information about your former members that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former members.** Exception: When you disclose the information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes [§1016.14] or
when one of the other exceptions apply. [§1016.15]. See EXCEPTIONS TO OPT OUT REQUIREMENTS later in this SUMMARY.

- **Service providers and joint marketing:** If you disclose nonpublic personal information to a nonaffiliated third party to perform services for you (which may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between the credit union and one or more financial institutions) - you must include a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted. You satisfy this disclosure requirement if you:
  
  o List the categories of nonpublic personal information that you disclose, with examples, and
  o State whether the third party is: (A) a service provider that performs marketing services on your behalf or on behalf of you and another financial institution, or (B) a financial institution with whom you have a joint marketing agreement.

- **An explanation of the consumer’s rights to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right.** The methods include: by mail, by electronic means or when the customer has an isolated transaction with the credit union, such as purchasing a cashier’s check, you provide the notice at the time of the transaction and request the consumer to decide before completing the transaction. [§1016.10(3)(iii)]

- **Any disclosures that you make under the Fair Credit Reporting Act** (regarding the ability to opt out of disclosures of information sharing among affiliates):

- **Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.** You meet this requirement if you: (a) describe in general terms who is authorized to have access to the information, and (b) state whether you have security practices and procedures in place to ensure the confidentiality of the information in accordance with your policy. You are not required to describe technical information about the safeguards you use; and

- **Whether you disclose nonpublic personal information to third parties as allowed in the EXCEPTIONS sections of the rule.** [§1016.14 and 15] You are not required to list the exceptions in the initial or annual privacy notices. It is sufficient to state
that you make disclosures to other nonaffiliated companies: (1) for your everyday business purposes, such as [include all that apply] to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus; or (2) as permitted by law.

If You DO NOT Disclose Nonpublic Information [Simplified Notices §1016.6(c)(5)]:

If you do not disclose, and do not wish to reserve the right to disclose, nonpublic personal information about members/consumers or former members/consumers to affiliates or nonaffiliated third parties, except for processing and servicing transactions or other allowed exceptions, you may simply state that fact, in addition to:

(a) the categories of nonpublic personal information that you collect,

(b) your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information, and

(c) a description of all nonaffiliated third parties that are subject to exceptions under the rule.

To satisfy this third requirement it is sufficient to state that you make disclosures to other nonaffiliated companies:

(1) for your everyday business purposes, such as [include all that apply] to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus; or

(2) as permitted by law. [§1016.6(b)]

Short-Form Initial Notice for Nonmembers [§1016.6(d)]: You may satisfy the initial notice requirements for nonmembers by providing a short-form initial notice at the same time you deliver an opt out notice. The short-form must:

(1) be clear and conspicuous,

(2) state that your privacy notice is available upon request, and

(3) explain a reasonable means by which the consumer may obtain the notice.

You are not required to deliver your privacy notice with your short-form initial notice. You may instead simply provide the consumer a reasonable means to obtain your privacy notice. You can do this by: (a) providing a toll-free telephone number that the consumer may call to request the notice, or (b) maintaining copies of the notice to provide immediately to consumers who conduct business in person at your office.

OPT OUT NOTICES [§1016.7]

May Combine with Initial Notice: You may provide the opt out notice together with or on the same written or electronic form as the initial notice.
When Opt Out Notice is Delivered After Initial Notice: If you provide the opt out notice later than required for the initial notice, you must also include a copy of the initial notice with the opt out notice.

When to Comply with an Opt Out Request: The credit union must comply with a consumer's opt out request as soon as reasonably practicable after you receive it. You may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer that you have collected, regardless of whether you collected it before or after receiving the request to opt out. [§1016.10(b)]

Partial Opt Out: You may allow a member/consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to the consumer's opt out request. [§1016.10(c)]

Continuing Right to Opt Out. A consumer may exercise the right to opt out at any time. The consumer's request to opt out is effective until the consumer revokes it in writing, or if the consumer agrees, electronically. A consumer's opt out request continues to apply to the nonpublic personal information that you collected during or related to membership or providing a service or product to a nonmember. If the individual later establishes a new member/consumer relationship with the credit union, the opt out request that applied to the former relationship does not apply to the new relationship.

Opt Out Notice for Joint Accounts If two or more members jointly obtain a financial product or service, other than a loan, the credit union may provide only a single opt out notice. The notice must explain how the credit union will treat an opt out request by a joint member. [§1016.7(e)]

Any of the joint members may exercise the right to opt out. You may either: (1) treat an opt out request by a joint member as applying to all of the associated joint members; or (2) permit each joint member to opt out separately. If you permit each joint member to opt out separately, you must permit one of the joint members to opt out on behalf of all of the joint members.

** You may not require all joint members to opt out before you implement any opt out request.

CONTENT OF OPT OUT NOTICES [§1016.7]
Using the Model Form meets the content requirements [§1016.7(K)]

Your opt out notice must state: (1) that you disclose or reserve the right to disclose nonpublic personal information about your consumer to a nonaffiliated third party, (2) that the consumer has the right to opt out of that disclosure, and (3) a reasonable means by which the consumer may exercise the opt out right.
You provide a **reasonable means** if you:

(A) designate check-off boxes in a prominent position on the relevant forms with the opt out notice,

(B) include a reply form together with the opt out notice - **in the case of privately insured credit unions**, you must include the address to which the form should be mailed,

(C) allow 30 days from the date you mailed the notices,

(D) if the consumer agrees to the electronic delivery of information, provide an electronic means to opt out, such as a form that can be sent via electronic mail or a process at your website, and allow 30 days from when the member/consumer acknowledges receipt of the notice, or

(E) provide a toll-free telephone number that consumers may call to opt out, and allow 30 days for the member/consumer to call.

An opt out method is considered **unreasonable** if:

(A) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right, or

(B) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that you provided with the initial notice but did not include with the subsequent notice.

**Adequate opt out notice:** You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you:

(A) identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose,

(B) identify all of the categories of nonaffiliated third parties to which you disclose the information,

(C) state that the consumer can opt out of the disclosure of that information, and

(D) identify the financial products or services that the consumer obtains from you, either singly or jointly, to which the opt out direction would apply.

**Specific Opt Out Method:** You may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.
REVISED PRIVACY NOTICES  [§1016.8]

You must not, directly or through any affiliate, disclose any nonpublic personal information about a member/consumer to a nonaffiliated third party other than as described in the initial privacy notice, unless:

1. You have provided a clear and conspicuous revised notice that accurately describes your policies and practices;
2. You have provided a new opt out notice;
3. You have given the member/consumer a reasonable opportunity, before you disclose the information, to opt out of the disclosure, and
4. The member/consumer does not opt out.

When a Revised Notice is not Required:  When you disclose nonpublic personal information to a new nonaffiliated third party that you adequately described in your prior notice – a revised notice is not required.

DELIVERING PRIVACY AND OPT OUT NOTICES  [§1016.9]

A credit union must provide all privacy notices and opt out notices, including short-form initial notices, so that each member/consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically. You may reasonably expect that a member/consumer will receive notice if you:

1. hand-deliver a printed copy of the notice to the member/consumer;
2. mail a printed copy of the notice to the last known address of the member/consumer;
3. for members who conduct transactions electronically, you must post the notice on the electronic site and require the member to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service, privately insured credit unions must post the notice “clearly and conspicuously”. [§1016.9(b)(1)(iii)(B)]
4. for isolated transactions, such as ATM transactions, post the notice on the ATM screen and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.

Retention or accessibility of notices for members:  You must provide the initial notice, the annual notice and the revised notice so that the member can retain them or obtain them later in writing or, if the member agrees, electronically.  [§1016.9(e)]
You may not deliver privacy notices by: (1) only posting a sign in a branch or office or generally publish advertisements of your privacy policies and practices, or (2) send the notice via electronic mail to a member/consumer who does not obtain a financial product or service from you electronically.

Verbal description of notice insufficient: A credit union may not provide any privacy related notice by orally explaining the notice, either in person or over the telephone.

Joint notice with other financial institutions: A credit union may provide a joint notice with one or more affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the credit union and other institutions.

Joint accounts: If two or more consumers jointly obtain a financial product or service, other than a loan, the credit union may satisfy the requirement for delivering the initial privacy notice by providing one initial notice to those consumers jointly. [§1016.9(i)]

For privately insured credit unions: If two or more consumers jointly obtain a financial product or service the credit union, the credit union may satisfy the initial, annual, and revised notice requirements by providing one notice to those members jointly, unless one or more of those members requests separate notices. [§1016.9(h)]

Special rule for loans [§1016.9(i)(2)]: A credit union is required to provide an initial notice to a borrower or guarantor on a loan if the credit union shares his or her nonpublic personal information with nonaffiliated third parties - other than for service providers, joint marketing, processing and servicing transactions, and other allowable exceptions under the rule. A credit union may satisfy the annual notice requirements by providing one notice to those borrowers and guarantors jointly.

EXCEPTIONS TO THE OPT OUT REQUIREMENTS [§1016.13]

Services done on your behalf: The opt out requirements do not apply when you provide nonpublic personal information to a nonaffiliated third party to perform service for you or functions on your behalf, if you:

(1) Provide the initial privacy notice; and
(2) Enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information, including use under an exception in §§1016.14 or 1016.15 in the ordinary course of business to carry out those purposes.

Joint Marketing: The services a nonaffiliated third party performs for you may include marketing of your own products or services or marketing of financial products or services offered through joint agreements between you and one or more financial

12
institutions. Joint agreement means a written contract in which you and one or more financial institutions jointly offer, endorse, or sponsor a financial product or service.

During the debate on new privacy rules, CUNA lobbied vigorously that it was unfair if any law were to pass that treated information sharing among financial conglomerates more favorably than information sharing that credit unions do with third parties such as CUNA Mutual. Because of CUNA’s efforts, an exception from the opt out requirements for “joint agreements” between credit unions and other financial institutions was added to the bill.

EXCEPTIONS §1016.14 and §1016.15

The requirements for the initial privacy notice, the opt out and for service providers and joint marketing do not apply:

§1016.14: if you disclose nonpublic personal information as “necessary to effect, administer, or enforce a transaction”* that a member or consumer requests or authorizes, in connection with:

(1) Servicing or processing a financial product or service that a member/consumer requests or authorizes;

(2) Maintaining or servicing the member’s account with you, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(3) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the member.

§1016.15: when you disclose nonpublic personal information -

(1) With the consent of the member/consumer,

(2) To protect the confidentiality or security of your records pertaining to the member/consumer, service, product or transaction;

(3) to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability;

(4) For required risk control or for resolving consumer disputes or inquiries,

(5) To persons holding a legal or beneficial interest relating to the member/consumer;

(6) To persons acting in a fiduciary or representative capacity on behalf of the member;
(7) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with industry standards, and your attorneys, accountants, and auditors;

(8) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act, to law enforcement agencies, a state insurance authority, self-regulatory organizations or for an investigation on a matter related to public safety.

(9) To a consumer reporting agency in accordance with the Fair Credit Reporting Act or from a consumer report from a reporting agency,

(10) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit;

(11) To comply with Federal, state or local laws, rules and other applicable legal requirements;

(12) To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, state, or local authorities, or

(13) To respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance or other purposes authorized by law.

* "necessary to effect, administer, or enforce a transaction" means that the disclosure is: (1) required, or is one of the lawful or appropriate methods, to enforce your rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or (2) required, or is a usual, appropriate or acceptable method: (a) to carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the member's account in the ordinary course of providing the financial service or financial product; (b) to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part; (c) to provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the member/consumer or their agent or broker; (d) to accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party; (e) to underwrite insurance at the member's request or for reinsurance purposes, or for any of the following purposes as they relate to a member's insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review
activities), participating in research projects or as otherwise required or specifically permitted by Federal or state law, or (f) in connection with (1) the authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit, or other payment card, check, or account number, or by other payment means; (2) the transfer of receivables, accounts, or interests therein; or (3) the audit of debit, credit, or other payment information.

WHAT HAPPENS WHEN YOU NO LONGER MEET AN EXCEPTION?

If you no longer meet the requirements of one of the exceptions listed in the rule because you have changed your policies or practices in such a way that you must provide a revised privacy notice, you will treat the revised privacy notice as an initial notice and provide an annual notice.

If you no longer meet the requirements of one of the exceptions in the rule because you changed your policies or practices in such a way that does not require you to provide a revised privacy notice, you must provide an annual privacy notice within 100 days of the change in your policies or practices that causes you to no longer meet the exception requirements.

When you once again meet an exception: You have changed your policies and practices in such a way that you no longer meet the requirements of one of the exceptions and, consequently, you have provided an annual notice to your members. After providing the annual notice to your members, you once again meet the requirements of for an exception to the annual notice requirement. You do not need to provide additional annual notices to your members until such time as you no longer meet the exceptions.

WHAT HAPPENS WHEN CONFIDENTIAL INFORMATION IS SHARED WITH YOU? [§1016.11]

Information you receive under an exception: If you receive nonpublic personal information from a nonaffiliated financial institution under one of the exceptions in §1016.14 and §1016.15 your use of that information is limited as follows:

(1) You may disclose the information to the affiliates of the financial institution that shared the information with you;

(2) You may disclose the information to your affiliates, but your affiliates may only use the information to the extent that you can use it;

(3) You may use the information as allowed by the exceptions in §1016.14 and §1016.15 in the ordinary course of business to carry out the activity covered by
the exception under which you received the information. (You cannot disclose the information to a third party for marketing purposes or use that information for your own marketing purposes. §1016.11(a)(2))

**Information you receive outside an exception:** If you receive nonpublic personal information from a nonaffiliated financial institution, other than under an exception in §1016.14 and §1016.15, you may disclose the information only:

(1) to the affiliates of the financial institution that shared the information with you;
(2) to your affiliates, but your affiliates may only use the information to the extent that you can use it;
(3) to any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information. This means you may disclose the information in accordance with the privacy policy of the financial institution from which you received the information, as limited by the opt out direction of each member whose nonpublic personal information you intend to disclose, and you may disclose the information in accordance with the exceptions listed in §1016.14 and §1016.15.

**Information you disclose under an exception:** If you disclose nonpublic personal information to a nonaffiliated third party under an exception in §1016.14 and §1016.15, the third party may disclose and use the information only as follows:

(1) the third party may disclose the information to your affiliates;
(2) the third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and
(3) The third party may disclose and use the information pursuant to an exception in §1016.14 and §1016.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

**Information you disclose outside of an exception:** If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in §1016.14 and §1016.15, the third party may disclose the information only:

(1) to your affiliates,
(2) to its affiliates, but its affiliates may only disclose the information to the extent the third party can disclose the information, and
(3) to any person, if the disclosure would be lawful if you made it directly to that person - taking into consideration your members' opt out directions.

**STATE LAW**

A state law, regulation, order or interpretation is not inconsistent with this federal privacy regulation if the protection under the state law, regulation, order or interpretation is greater.