



Online Lenders Alliance

**Best Practices**

**March 2016**

## OLA Consumer Hotline



The OLA Consumer Hotline provides a resource for consumers to speak to live operators for help and to report fraud. The Hotline helps consumers by allowing them to hear a reassuring voice, tell their stories, and resolve simple issues quickly.

OLA encourages all members to display the consumer hotline number on their websites to ensure OLA is the go-to resource for consumers.

**Consumer Hotline Number:**  
**1-866-299-7585**

# Look for the Seal



When you see the OLA seal, you can trust you're working with a company committed to the highest standards of conduct, dedicated to ensuring the best possible experience for their customers, fully compliant with federal law, and working hard to protect consumers from fraud.

Embedding the seal will ensure no company can falsely display the OLA logo on websites. To receive the OLA embedded logo, please send all company names and website addresses to Liz Jones. We'll send your IT team instructions for implementation.

The OLA Member logo will not appear if your URL is not on file with OLA! Please send all your DBAs to OLA at [contact@oladc.org](mailto:contact@oladc.org)

## **Policing the Industry**

OLA is a self-policing organization and takes compliance very seriously. In order to become a Member of OLA, you need to certify that you are in compliance with our Best Practices.

One of the ways that OLA Monitors fraudulent activity is through our complaint process, which covers the entire online lending ecosystem, not just OLA Members.

Once a complaint is submitted, The OLA Board via its Standards Committee will review all reported violations of the Best Practices and will direct the OLA Member, or Company that is the subject of the report to address the issue in accordance with the guidelines set forth herein.

Those who are receiving the Notice has 14 business days from receipt of the Notice to contact OLA in writing for an opportunity to defend the claim, practice or other representation or action.

The OLA Standards Committee will review this response and will make a final determination of whether a violation of the Best Practices occurred within 5 business days of receipt of the Member or Company's response.

Those who believe an OLA Member, or Company is in violation of our Best Practices can email: [complaints@oladc.org](mailto:complaints@oladc.org) for a copy of our complaint form.

# Table of Contents

|  |    |
|--|----|
| Introduction .....                     | 1  |
| Overarching Guidelines .....           | 2  |
| OLA Code of Conduct .....              | 2  |
| Requirements of Membership .....       | 3  |
| Implementation of Best Practices.....  | 4  |
| OLA Antitrust Statement.....           | 5  |
| Self-Regulatory Principles .....       | 6  |
| OLA Best Practices                     |    |
| Advertising & Marketing .....          | 8  |
| Best Practices                         |    |
| Application and Origination .....      | 14 |
| Best Practices                         |    |
| Security of Information .....          | 18 |
| Best Practices                         |    |
| Payment Processing .....               | 20 |
| Best Practices                         |    |
| Collections Best Practices.....        | 24 |
| Mobile Best Practices .....            | 30 |
| Vendor Selection and .....             | 43 |
| Compliance Best Practices              |    |
| Appendices                             |    |
| Definitions .....                      | 45 |
| Federal Laws And Regulations .....     | 46 |
| Validation of Routing Numbers.....     | 48 |
| Electronic Payment Authorization ..... | 49 |
| Vendor Agreement .....                 | 50 |

# Introduction

The Online Lenders Alliance (OLA) believes sound business practices and objective standards are essential to ensuring industry excellence and longevity. To that end, OLA has developed detailed Best Practices for all Members to use in their businesses. Unless stated otherwise, the Best Practices described herein apply to all entities involved in the marketing, origination and collection of a Loan. This includes Lenders, Vendors, Affiliates and any other third parties doing business with a Member to market, originate, service and/or collect on the Loan. As a Member, you are responsible for ensuring that any Lenders, Vendors, Affiliates, and any other third parties with whom you do business comply with these Best Practices, regardless of whether the third party is also a Member.

By following these Best Practices, every Member will enhance its customers' experience and promote a positive reputation for the industry. These cohesive standards will ensure customers have a transparent and quality experience.

The Best Practices are organized as follows:

- I. **General:** Overarching guidelines.
- II. **Advertising & Marketing:** How to appropriately communicate with current and potential customers.
- III. **Application and Origination.** How to originate Loans that are legally compliant and fully transparent to customers.
- IV. **Payment Processing:** How Members retrieve payments and prevent fraud.
- V. **Collections:** How to fairly manage collections on past due accounts.
- VI. **Data Security:** How to protect Consumer information.
- VII. **Vendor Selection:** How to select and interact with third party vendors.
- VIII. **Implementation.** How to implement and maintain these Best Practices.

OLA encourages Members to interpret and apply these Best Practices broadly and in a manner that protects customer interests to the maximum extent possible.

One of OLA's main missions is to provide continuing education for Members to help ensure that they are apprised of current regulatory changes as well as the most up-to-date business practices. Members are offered regular programs and forums for discussion of best practices and sharing of business practices.

## **OLA Best Practices – Overarching Guidelines**

- Ensure Consumers are making educated financial decisions by fully disclosing all Loan terms in a transparent and easy to understand way.
- Give Consumers a chance to change their mind by maintaining a reasonable cancellation policy.
- Be a company in good standing with the officials and regulatory bodies that govern you. Comply with all applicable laws and regulations.
- Never engage in activities that are unfair, abusive or deceptive.
- Protect every Consumer's personal data with comprehensive website security and a privacy policy and ensure that your Vendors protect Consumer personal data in the same manner.
- Provide Consumers with a copy of your privacy policy and an ability to opt out of information sharing.
- Help Consumers help themselves by providing referrals to credit counseling, education and assistance when appropriate.
- Use advertising and marketing practices that promote the responsible use of short-term credit services. Do not engage in any false, misleading or deceptive advertising campaigns.
- Take applications from Consumers and originate Loans consistent with all applicable laws
- Ensure that payments are authorized and processed consistent with federal laws and that Consumers fully understand the options for sustained use of Loans.
- Provide comprehensive website security and fraud prevention practices that include timely and accurate reports on loan activity, consumer notification of account use, and validation of routing numbers.
- Always treat consumers with respect and use fair, professional and non-abusive collection practices. Never use unlawful threats, intimidation, or harassment to collect accounts.
- Appropriately manage third-party service providers to ensure that consumer information is shared and protected consistent with applicable law

## **OLA Code of Conduct**

Treat people fairly and with respect.

## **Requirements of Membership**

To qualify for membership in OLA a company must:

1. Certify that it complies with these Best Practices;
2. Adhere to OLA's Antitrust Statement and comply with all federal and state antitrust laws;
3. Adhere to the Self-Regulatory Principles; and
4. Comply with all other applicable federal and state laws.

In the event of a conflict between these Best Practices and any federal and/or state law or rule, the applicable law or rule applies.

These Best Practices are not intended to substitute for legal compliance and there may be other laws and regulations applicable to your business activities that are not covered in these Best Practices. Moreover, federal and state laws in this area change frequently. Members must continually monitor applicable laws, regulations, guidelines, and principles in consultation with capable counsel as necessary, to ensure that your business activities stay within the bounds of the law.

OLA is a self-policing organization. If OLA discovers or receives a report of any violations of the Best Practices, Antitrust Statement or Self-Regulatory Principles, the OLA Board of Directors will take immediate action. The OLA Board will investigate the reported violations and will request and direct that the OLA Member address the issue immediately. The Board will monitor the Member to ensure future compliance. The Board has the authority to suspend and terminate membership if any Member is found to be in violation of any Best Practices, the Antitrust Statement or Self-Regulatory Principles.

**NOTHING CONTAINED IN THIS DOCUMENT SHOULD BE  
CONSTRUED TO CONSTITUTE LEGAL ADVICE.**

## **Implementation of Best Practices**

Adoption of these OLA Best Practices requires that Members undertake steps to ensure that all parties – from third party Vendors to employees are aware of the requirements.

Accordingly, Members must evidence that these Best Practices are part of their business day-to-day activities. This means that the Member must ensure that these Best Practices are:

- Reflected in new hire trainings and employee manuals.
- A prominent part of any training classes.
- Incorporated as part of the Member's formal policies.
- Reflected in agreements with third party Vendors.

OLA Members also must establish procedures for handling complaints. These procedures must ensure that all employees are aware of the Best Practices and are acting in conformance therewith. OLA Members must identify at least one employee who is dedicated to resolving and tracking complaints and ensuring that the complaints are handled consistently with these Best Practices. OLA Members must maintain complaint logs that identify the nature of the complaint, the timeframe until resolution and the ultimate resolution.

## **Online Lenders Alliance Antitrust Statement**

It is the Online Lenders Alliance's (OLA) policy to comply with both federal and state antitrust laws. Our aim is to conduct ourselves in such a way as to avoid any potential for antitrust exposure.

Full compliance with the antitrust laws is a requirement for OLA membership, and responsibility for compliance rests with each Member.

Competitors should not discuss certain subjects when they are together — either at formal association meetings or during informal contacts with other industry members. Topics to avoid discussing with competitors include: prices, costs of common inputs, margins, terms of sale, discounts and rebates, promotional programs, inventory levels, production levels, capacities, new projects, and the like.

Further, with rare exceptions that should be made only upon the advice of counsel, Members may not:

- Fix or set prices for selling products or services;
- Allocate geographic markets or customers between or among competitors;
- Boycott competitors, buyers, classes of buyers, or suppliers;
- Conspire to exclude competitors or suppliers from the market;
- Rig bids, rotate bids, or otherwise distort the bidding or contracting process;
- Agree upon levels of supply to the marketplace; or
- Discuss specific sales or marketing plans, R&D, or any company's confidential strategies.

OLA meeting participants have an obligation to terminate any discussion, seek legal counsel's advice, or, if necessary, terminate any meeting if the discussion might be construed to raise any antitrust risks.

## Self-Regulatory Principles

Inspired by the self-regulatory principles adopted by many online advertisers as memorialized in: “Self-Regulatory Principles for Online Behavioral Advertising” (the “OBA Principles”),<sup>1</sup> the OLA adopts the following principles, which apply broadly to all Members.

In response to calls by the FTC on the online advertising industry to develop self-regulatory principles for online behavioral advertising, industry released the OBA Principles to promote enhanced transparency and consumer control. The OBA Principles are seven-fold and address: education, transparency, consumer control, data security, material change, sensitive data, and accountability. Although the OBA Principles are not a perfect match for the online short-term lending industry, the similarities between the industries motivated OLA to adopt the principles stated below for its Members.

- **The Education Principle.** This principle calls for entities to participate in efforts to educate consumers regarding short term online lending practices.
- **The Transparency Principle.** This principle requires clear disclosure to consumers about data collection and use in the online short term loan origination process – from the time a lead is taken to the time that the consumer receives funds.
- **The Consumer Control Principle.** This principle permits consumers to choose whether data is collected and used or transferred to a non-affiliate for such purposes.
- **The Data Security Principle.** This principle requires entities to provide reasonable security for, and limited retention of data collected and used for short term loan origination purposes.
- **The Material Changes Principle.** This principle directs entities to obtain consent before applying any change to their online data collection and use policy that is less restrictive to data collection prior to the material change.

---

<sup>1</sup> A copy of the Report is available here: <http://www.aboutads.info/>

- **The Sensitive Data Principle.** This principle recognizes that certain data collected and used merits different treatment. As such, this principle requires consent for the collection of financial account numbers and Social Security Numbers.
- **The Accountability Principle.** This principle is intended to ensure that all entities engaged in online short term lending and that are Members of OLA bring their activities into compliance with the principles identified above.

We view these principles as overarching guidelines for OLA Members and require that each Member adhere to each of the above-identified principles as a requirement of membership.

## **Advertising & Marketing Best Practices**

OLA's goal is to enhance the consumer experience and promote the industry's reputation by establishing cohesive standards that ensure quality services, advertising and marketing. The Advertising & Marketing Best Practices are intended to provide Members, their Affiliates and any third party advertising a Member's products or generating leads for a Member with guidance regarding basic legal and ethical requirements for the promotion of lending products.

It is OLA's position that illegal, deceptive, or misleading communications negatively impact the industry as a whole and the customer experience.

By following these Best Practices we can ensure each Customer has the tools and information to make the decision best for their personal needs.

### **ACTUALLY AVAILABLE CREDIT**

For any advertisement of consumer credit, including a short-term loan, the advertisement must be accurate and only offer credit terms that are actually available. For example, if a Lender only makes Loans up to a dollar value of \$1,000, then neither it – nor any Affiliate advertising on the Lender's behalf - can advertise Loans in dollar values in excess of that threshold. The Lender also should make accurate representations regarding any repayment options that may be available to the Consumer. Given the nature of the marketplace, and our understanding of the credit offered by our Members, most OLA Members should not advertise credit in excess of \$1,000. Those OLA Members who do advertise credit in excess of \$1,000 should do so only if the Members will make loans in that amount to consumers.

Lead Generators and other third party entities that advertise Loans for multiple Lenders must also ensure that their advertisements describe Loan terms that are actually available from a participating Lender. [Again, if none of the Lenders working with a Lead Generator offer Loans in excess of \$1,000, then that Lead Generator cannot advertise that product.]

Additionally, advertisements should accurately inform consumers regarding when credit will become available. Typically, this means that advertisements should reflect that cash will be available to the consumer the "next day." Representation regarding cash in "one hour" or "same day" should [typically] not be made since Lenders will not be able to provide access to cash that quickly.

Finally, if a Lender will engage in a credit check before offering credit, then the advertisement must state that fact. It is acceptable to advertise that Loans are available for consumers with varying degrees of credit-worthiness, provided that the Consumer is made aware that the Lender will conduct a credit check. Note that a credit check can be offered by any entity that is a credit reporting bureau as defined under the Fair Credit Reporting Act, which definition is not limited to the “big three” credit bureaus (TransUnion, Experian and Equifax). Accordingly, advertisements should include a disclosure that Lenders will run credit checks via specialized credit bureaus. Advertisements should not include the phrase “No Credit Checks.”

### **TRIGGER TERMS**

To comply with the federal Truth in Lending Act, Lenders and their Affiliates must ensure that all advertisements contain all applicable disclosures. Thus, if an advertisement for a Loan contains a “trigger term,” then the advertisement also must contain certain required disclosures.

The trigger terms for closed-end loans under TILA are:

- The amount or percentage of any down payment.
- The number of payments or period or repayment.
- The amount of any payment.
- The amount of any finance charge.

Examples of trigger terms in advertisements include:

- Borrow now for just \$10 per \$100!
- Only [x]% interest!
- Get money now, pay back over the next 12 weeks!

Any advertisement that includes a trigger term must provide the following disclosures:

- The amount or percentage of the down payment.
- The terms of repayment.
- The annual percentage rate using that term.
- If the rate may be increased after consummation, the fact of that increase must be disclosed.

Different trigger terms and disclosures apply for Loans structured as open-end loans. If a Lender offers open-end Loans, then it must provide the relevant disclosures in its advertisements for that product.

## **LOAN TERMS**

OLA RECOMMENDS THAT ADVERTISEMENTS INFORM CONSUMERS ABOUT THE TERMS OF CREDIT AVAILABLE. ACCORDINGLY, THE FOLLOWING TOPICS SHOULD BE ADDRESSED IN ALL ADVERTISEMENTS:

- **Implications of Late Payments.** Consumers should be made aware that making late payments could result in late fees as well as collection activities. As such, advertisements for credit should contain the following, or substantially similar, disclaimer: “Late payments of loans may result in additional fees or collection activities, or both. Each Lender has their own terms and conditions, please review their policies for further information.”
- **Implications of Non-Payment.** Consumers also should be made aware that non-payment of a loan could result in collection activities. Accordingly, advertisements should provide the following, or a similar, warning: “Non-payment of credit could result in collection activities. Each Lender has their own terms and conditions, please review their policies for further information.”
- **Sustained Use.** Consumers should be aware that Lenders may renew or extend existing credit; and advertisements should inform consumers that: “Every Lender has its own renewal policy, which may differ from Lender to Lender. Please review your Lender’s renewal policy.”
- **Responsible Lending Policy.** Each advertisement should advise consumers that OLA Members adhere to the OLA Responsible Lending Policy.
- **Compliance with Applicable Law.** Each advertisement should assure consumers that OLA Members promise to comply with all applicable federal law to qualify for Membership in OLA.

## **TELEMARKETING COMPLIANCE**

Federal and state law regulates the actions of telemarketers. As such, OLA Members must comply with applicable provisions of the Telephone Consumer Protection Act (“TCPA”), Federal Communications Commission rules implementing the TCPA, the Federal Trade Commission’s Telemarketing Sales Rule, and other federal and state laws governing telemarketing. Without limiting the foregoing compliance requirement, Members who are telemarketers must:

- Abide by federal and state rules requiring the use of federal, state, and in-house “Do Not Call” lists.
- Only solicit between the hours of 8 a.m. to 9 p.m., local time (or as otherwise specified under more restrictive state law).
- Provide their name, the name of the person or entity on whose behalf the call is being made, and a telephone number or address at which that person or entity may be contacted.
- Not make solicitation calls to residences with artificial voices or recordings except as permitted by law.
- Abide by Federal Communications Commission rules for calling cell phones.
- Not send any unsolicited faxes.
- Comply with other requirements as specified by law.

### **INTERNET/E-MAIL MARKETING**

All marketing e-mails sent by an Advertiser must be fully compliant with the CAN-SPAM Act of 2003, Federal Trade Commission and Federal Communications Commission rules implementing CAN-SPAM, and applicable state laws. Although the federal CAN-SPAM Act preempts many aspects of state anti-spam laws, it does not generally preempt state laws that prohibit fraud or deception in e-mail marketing practices.

All “commercial” messages sent by an Advertiser are subject to CAN-SPAM. CAN-SPAM defines a “commercial” e-mail to include any message that has the primary purpose of advertising or promoting a commercial product or service, including content on an Internet web site operated for a commercial purpose. There is no exemption for commercial messages sent to persons with whom the sender of the message has an existing business relationship. Members should consult legal counsel if you are unsure about whether a particular type of e-mail message is subject to CAN-SPAM requirements.

CAN-SPAM compliance requirements are as follows:

- Do not use false headers. “Header” information includes source code, destination code, routing information and other information related to the transmission of the message.

- Do not use a deceptive or misleading “from” line.
- Include a relevant, non-misleading “subject” line that accurately describes the contents of the message.
- Include a postal address for the “sender” of the message. “Sender” refers to the party whose products or services are promoted in the message.
- Include a visible and functional “unsubscribe” mechanism that allows the recipient to request not to receive future commercial message from the “sender” of the message.
- Honor all opt-out requests within 10 days of receipt.
- Prior to sending an e-mail campaign, “scrub” the distribution list against any list(s) of individuals who previously requested not to receive commercial messages from the “sender.”
- Advertiser opt-out lists may be used only for CAN-SPAM compliance purposes and may not be shared with or transferred to any third party for any purpose.
- Advertisers are responsible for ensuring that their own practices as well as the practices of their Lead Generators, and other third parties, are in compliance with the CAN-SPAM requirements, which includes the proper use and management of opt-out lists.

All advertisements made on the Internet must provide for a phone number and physical address for the person responsible for the advertisement (the Website owner).

#### **PUBLICATION OF TERMS AND CONDITIONS.**

- Members who engage in advertising and/or marketing, or who use Affiliates to advertise or market on their behalf, must post on their websites clear and conspicuous terms and conditions that describe the services provided by the Member. No text, graphics, or other marketing materials used by the Affiliate should contradict any aspect of the terms and conditions. An Affiliate who is NOT also a Lender should also conspicuously state that it does not actually provide short-term loans but refers Consumers to Lenders who may provide such loans.
- It will share Application information provided by the Consumer with one or more Lenders.

- It cannot guarantee that it will match a Consumer with a Lender, or that the Consumer's Application will be approved by a Lender.
- It cannot guarantee the amount of funds that may be extended to the Consumer if any Lender approves the Consumer's Application.
- The Lender may perform a credit check. Consumers should be informed that Lenders may perform a credit check or otherwise verify the Consumer's social security number or other information.

## **PROHIBITION ON SELLING BANK ACCOUNT AND SSN INFORMATION**

- SSN and bank account information collected from consumers on a lending website or in connection with a loan request or application, may not be used or disclosed to any third party except where a lead generator provides such information to a lender or to a lender's lead management service for the purpose of helping the consumer obtain a loan.

# **Application and Origination Best Practices**

## **PRIVACY NOTICE**

Consistent with the Gramm-Leach-Bliley Act, all financial institutions, which term includes Lenders and arguably also includes Lead Generators, must provide Consumers with notice of the entity's privacy policies. If the entity will share the Consumer's nonpublic financial information with non-affiliated parties, then the entity must give the Consumer the ability to opt out of that sharing. Lead Generators, unlike Lenders, do not have "customers" as that term is defined under Gramm-Leach-Bliley, and, thus, will not be required to provide annual notice of its privacy policies.

## **ADVERSE ACTION NOTICES**

Generally speaking, according to the Equal Credit Opportunity Act ("ECOA"), a Lender is required to notify any applicant for a Loan of action taken on the Application (denial or approval) within 30 days of receiving a completed Application. An "adverse action" includes refusing to grant a Loan in substantially the amount or on substantially the terms requested in the Application, unless the Lender makes a counteroffer and the Applicant uses or expressly accepts the Loan offered.

Whenever a Lender takes an adverse action, it must provide, in writing, a notice of adverse action and a statement of the specific reasons for the adverse action (*e.g.*, insufficient credit score, creditor's internal standards or policies, *etc.*) or direction to the consumer to request the statement of specific reasons. ECOA provides for model adverse action forms that, when used by a Lender, are a safe harbor for compliance (these forms are applicable to either format – by providing a checklist of specific reasons or by informing the consumer of his right to request the reasons) .

Notwithstanding the above, when an applicant applies for credit via a third party (such as a Lead Generator), then the onus for providing any applicable adverse action notices to that applicant can reside with the Lead Generator. Specifically, Regulation B provides for special rules when an Application for credit is provided to multiple Lenders. In such cases, when a Lead Generator submits an Application for credit to more than one Lender, and the applicant expressly accepts or uses credit offered by one of the Lenders, none of the other Lenders who received the Application and denied it is required to provide an adverse action notice.

If, however, no Lender extends credit, or if the applicant does not expressly accept or use any credit offered, each Lender taking adverse action must provide notice of the adverse action directly or through the Lead Generator. A notice given by a Lead Generator must disclose the identity of each Lender on whose behalf the notice is given. Accordingly, the Lender could amend its Vendor agreements with its Lead Generators to place the onus on the Lead Generator to provide this notice. The Lender also will need to create some policies and procedures to support this practice.

The Fair Credit Reporting Act ("FCRA") also contains an adverse action notification requirement similar to the requirement described above under ECOA. FCRA applies when the Lender bases its decision to deny credit in whole or in part on information from a source other than its own files. ECOA's model forms also can be used to comply with FCRA's adverse action notice requirements.

## **DISCLOSURE OF LOAN TERMS**

According to the federal Truth in Lending Act, all Lenders must disclose the appropriate information for the loan type originated (*i.e.*, closed-end disclosures for closed-end loans and open-end disclosures for open-end loans.). For closed-end loans, these disclosures include the Annual Percentage Rate, the Finance Charge, the Total of Payments, and the Payment Date and Amount. For open-end loans, different disclosure requirements apply. For closed-end loans, the required disclosures must be grouped together and segregated from the loan agreement and terms. For open-end loans, the disclosures may be included as part of the loan agreement.

In either case (open- or closed-end) the disclosures must reflect the legal obligation of the Consumer. Said differently, the disclosure must accurately reflect the term, cost and repayment obligations to which the Consumer is bound. For example, if a Lender requires repayment in one lump sum at a designated date, the disclosures must reflect that. In contrast, if a Consumer agrees to an installment-based repayment plan, the disclosures must reflect that repayment plan.

## **ELECTRONIC PAYMENT AUTHORIZATION**

Lenders must ensure that they obtain the appropriate type of authorization to initiate electronic payments for the repayment option appropriate for the Loan. Lenders must obtain these authorizations consistent with the requirements of the Electronic Funds Transfer Act and the NACHA Guidelines (note that the EFTA will apply to all electronic fund transfers but NACHA will apply only to ACH transactions processed through the ACH system). Note that the EFTA expressly prohibits the conditioning of credit on repayment via recurring electronic debits. As such, Loan documents should expressly permit Consumers to repay via a method other than a recurring debit. Lenders are, however, permitted to incentivize Consumers to repay electronically via price breaks.

- **One Time Debit.** Lenders must provide Consumers of notice that a one-time debit will be made to the Consumer's account. The Consumer must be aware of the amount of the debit and the date on which it will be withdrawn from the Consumer's account. Notice provided in the loan agreement is sufficient to meet this requirement.
- **Recurring Debits.** Lenders must obtain written authorization to initiate recurring debits to a Consumer's account. This authorization may be for a specific dollar amount (i.e., \$10) or it may be for a reasonable range of amounts (i.e., \$10 - \$20). Any time that the debit amount will vary from the authorized amount, then the Lender must send timely notice notifying the Consumer of the different debit amount. In addition to the amount of the debit, the Consumer must know the dates on which the debit will occur. Written authorization can take the form of a paper writing or an electronic authorization. Irrespective of the method used, the Lender must retain copies of the authorization and provide the Consumer with a copy of the authorization. A sample authorization is included in the Appendix to this Best Practice.

For any electronic payments that are processed through the ACH system, the Lender must ensure that the "Company Name" field clearly contains the name of the Lender, which is known to and readily recognized by the Consumer. Processors should have the ability to put "dba" names in the company identification field.

Lenders and their Processors should create policies and procedures to ensure that unauthorized debits are not initiated, and, if they do occur, are quickly identified and reversed.

## **COUNSELING**

For those Consumers who may find themselves unable to repay their Loan or who may need financial counseling prior to obtaining a Loan, the Lender should be prepared to make referrals to nearby financial counselors.

## **DATA PASSING/NEGATIVE OPTIONS**

In response to growing consumer concern that unauthorized third parties were using their personal financial information submitted for purchases made online, Congress adopted the “Restore Online Shoppers Confidence Act.” The Act prohibits online data passes and regulates the use of online negative option marketing. The implications of this Act are important for any Lender who solicits customers online via the use of a Lead Generator or other third party Vendor. Specifically, Lenders should ensure that any potential Loan applicants receive clear disclosures and fully understand their relationships with all parties engaged in the offering and origination of a Loan:

- Before obtaining an applicant’s financial information, the Lead Generator or Vendor should clearly and conspicuously disclose that it is not affiliated with the Lender and that any offer by the Lead Generator or Vendor will result in separate charges unrelated to the cost associated with obtaining a Loan.
- The applicant must affirmatively consent to purchasing a service unrelated to the Loan. This affirmative consent can occur via clicking a confirmation button or checking a box.
- The applicant must receive clear and conspicuous disclosure of all material terms of any service purchased including (if relevant): (i) that the customer will be charged a specified amount on a recurring basis until the Applicant cancels the service; (ii) that the amount charged may change, and the amount of any change (if known); (iii) the date on which the Applicant will be charged; (iv) the date by which the Applicant must cancel to avoid future charges; (v) the seller’s refund policy; and (vi) minimum purchase obligations.
- If the offer contains a free trial period, that fact along with the date and time by which cancellation must be received to avoid charges, must be disclosed.

# Security of Consumer Information Best Practices

## COLLECTION OF INFORMATION

OLA Members understand the importance of having and maintaining data security and information privacy. Accordingly, OLA Members must have a solid understanding of their business processes around the collection and maintenance of Consumer Information.

OLA Members must validate on a regular basis (at least one time per year or as required by law) that their security process and procedures provide reasonable protection against system intrusion and theft. OLA Members also must communicate clearly with all Customers and business entities with respect to the way in which customer information is shared with other entities by having a stated privacy policy on all websites owned/operated by the Member conspicuously placed on the website.

All Personally Identifiable Information collected from Consumers should, at a minimum, be collected utilizing the following procedures:

- Collect information using a Hypertext Transfer Protocol Secure (https) connection or other connection that provides at least the same level of protection.
- Store Consumer Information only in an encrypted, unreadable format.
- Employ readily available security measures to guard against reasonably foreseeable attacks, such as Structured Query Language injection attacks.
- Use readily available security measures to monitor and control connections from its database of Consumer data to the internet.
- Employ reasonable measures to detect unauthorized access to Consumer information.
- Retain data only as long as is necessary to satisfy a legitimate business, law enforcement, or other legal need.

- Limit the number and types of third parties with whom such information may be shared in order to minimize, to the best extent possible, security risks to Consumer data that is outside the control of the Member. Such limitations may require contractual agreements or similar requirements.
- Designate at least one employee to oversee and be responsible for the information security program.
- Identify material security risks and assess the sufficiency of any safeguards in place to control information security risks.
- Design and implement reasonable safeguards to control the identified security risks, and regularly test or monitor the security measures implemented.
- Evaluate and adjust an information security program on an ongoing basis.
- Denote at least one employee to manage the safeguards.
- Construct a thorough risk management process in each department for handling the nonpublic personal information.
- Develop, monitor, and test a program to secure the information.
- Change safeguards as needed with the changes in how information is collected, stored, and used.
- In instances of alleged identity theft, fraud or mistaken identity, conduct a reasonable investigation to determine the validity of the debt, the identity of the obligor on the account and the accuracy of the information in the possession of the Member.

Members need to ensure that the sharing of Consumer Information in the course of the origination of a Loan is conducted consistent with the applicable privacy policies of each entity that collects Consumer Information. More specifically, Members are not allowed to obtain or share information where the Consumer is not given an appropriate opportunity to opt out of the information sharing. And, unless the Consumer obtains a Loan from the Member, the Member is prohibited from utilizing any Consumer Information obtained about the Consumer for marketing purposes.

## **Payment Processing Best Practices**

OLA members ascribe to ensure that customer debits and credits are done in a timely and customer friendly manner.

### **Consumer Rights**

Lenders shall provide consumers an alternative to ACH debiting. These alternatives shall be provided both when the customer is current and in collection stages. Such alternatives may include paper check, debit card, money order, or other means.

All customers must have the right to rescind the loan and the ACH authorization within one (1) business day of the loan approval so long as the customer returns the funds within 24 hours of the rescission.

Lenders will not process multiple ACH debit attempts to an individual loan on the same effective date (No ACH Split Payments) unless expressly authorized by (expressly requested by) the customer.

### **Lenders Responsibilities to Consumers**

Lenders will follow all NACHA presentment rules – one original presentment plus only two re-presentments on each original payment.

Lenders shall charge only one NSF fee per original loan payment.

### **REPORTING**

All authorizations for recurring debits shall be secured in accordance with NACHA rules, the Electronic Funds Transfer Act and Regulation E. This shall include securing authorization for recurring debits in writing and signed or similarly authenticated by the consumer:

1. Authorization can be electronic
2. Authorization must be retained and a copy provided to borrower
3. Must include the five essential elements defined by NACHA rules

All parties will comply with the new NACHA Rule 2.3.4 which requires the ODFI to ensure that originators and third-party senders do not share account/routing numbers for the purpose of initiating debit entries that are not covered by the original authorization.

Lenders shall transfer PII data using TPS and TPP security protocols to ensure no inappropriate passing of data.

## **REPAYMENT OPTIONS**

Lenders shall not ACH debit a consumer unless they have a valid authorization with the proper ABA and account information. Lenders shall not use new bank account information that the merchant sourced from the marketplace on the consumer, or in other words, Lenders shall only debit consumers for the account listed on the valid authorization.

Lenders shall not use RCCs and RCPOs in their normal course of business unless formally requested and proper consumer authorization has been secured.

Lenders shall provide their payment processors and the sponsoring ODFI signed payment authorizations for all R10's and R29's returns within 24 hours of the request for such documentation.

Lenders shall provide Proof of Authorizations to be delivered to TPP within 24 business hours of the request.

Lenders shall maintain all Proof of Authorization for all unauthorized transactions in a segregated manner and shall be delivered to TPP within 4 business hours, upon request.

## **TIMELY POSTINGS of Returns**

Lenders, processors and their agents shall develop and maintain timely posting of returns information.

## **RETURNS TESTS**

### General Guidance

Any merchant's (lender's) third party processor has the ultimate responsibility and authority to establish, monitor and adjudicate the rate of returns of all types and codes. The processor is the gateway to the ODFI bank partner and obligated to comply not only with federal regulatory standards but those established by NACHA. Notwithstanding this ultimate authority, both merchants (lenders) and processors are well advised to closely jointly monitor return rates of all types on a constant and continual basis. In the event a merchant's processor or bank does not frequently, proactively provide return code analysis by ABA, merchants (lenders) should ask their processor to do so on a monthly basis, and to review those data with recommendations to control return rates under levels acceptable to NACHA.

## Testing

Lenders/Merchants shall at a minimum test their portfolios monthly to generate the results of the previous month using the following tests on the next few pages. In the event that any merchant is out of the best practice realm they should work closely with their processor(s) and internal staff to correct lack of compliance swiftly. Regulators, Processors and other payment experts recommend daily and weekly review of these thresholds. They feel that not only will it make the relationship better with processors and ODFI but also make the product better for consumers and in some cases reduce default and fraud.

Test 1: The total count of all returns (all codes) shall not be greater than 30% of total debits processed as computed by the effective dates of the corresponding debits.

Test 2: The total count of all NSF Returns (R01 & R09) shall not be greater than 25% of total debits processed as computed by the effective dates of the corresponding debits.

Test 3: Lenders shall have an administration return code less than or equal to 4.0% of total debits processed as computed by the effective dates of the corresponding debits. Admin  $\leq$  4% (R02, R03, R04)

Test 4: All R05, R07, R10, R29, and R51's (negative chargeback returns) shall not to be greater than 0.5% of total debits processed as computed by the effective dates of the corresponding debits. (It is understood that NACHA's current requirement is 1.0% or less than)

Test 5: Lenders shall have a corrections (C Codes) of less than or equal to 0.40% of total debits processed as computed by the effective dates of the corresponding debits.

Corrections  $\leq$  0.40% (any C code).

Test 6: The total of all R01 and R09 (insufficient fund returns) shall be greater than 75% of the total returns for the merchant as computed by the effective dates of the corresponding debits.

Test 7: Lenders shall review individual ABA numbers which have an extremely high return percentage of the total transactions processed during any given thirty day period. For any ABA numbers that represent greater than 1.5X the merchants average return % (ABA returns vs. ABA debits) and if the merchant submitted more than 15 returns per month with the said ABA then Lenders will take the following measures:

1. Closely evaluate the applicant pre-approval, risk management and underwriting means and methods being used in comparison the industry best practices and the state of the art methods available from third party providers of consumer data, and promptly institute such improved measures.
2. Discuss with the processor recommendations for controlling returns.
3. In the event return rates do not fall into line with industry practices and NACHA guidelines, the lender is advised to cease funding loans from any such ABA

Test 8: Lenders shall review and promptly modify their approval and risk management practices for any individual ABA numbers for which more than 15 returns have been processed during the prior calendar month in order to ensure no single ABA number represents negative chargeback returns greater than 1.5% of total debits for said ABA as computed by the effective dates of the corresponding debits.

# Collections Best Practices

OLA's Collections Best Practices provides guidelines and direction to members in the recovery of delinquent Loans while ensuring compliance with all laws and regulations. These Best Practices assist Members to establish policies and procedures to assist with building positive and professional relationships with customers and communities. They promote compliance and self-regulation efforts to the highest level.

These guidelines apply to all Members.

Member companies need to ensure compliance with any non-Member company, including Vendors, agencies, buyers, contractors, *etc.*

## GENERAL STANDARDS

Members and their Vendors agree to:

- Cooperate and abide by the OLA's Best Practices.
- Treat consumers owing debts with professionalism, respect, and civility.
- Require all employees, agents, and contractors who attempt to collect debt to be FDCPA compliant, and conduct or receive ongoing FDCPA training.
- Comply with all applicable laws.
- Hold all necessary licenses, bonds and insurance coverage as required to collect the debt.
- Maintain network and data security and/or encryption to protect consumer information.
- Cease communication with consumers as required by applicable law when the consumer: (i) disputes the debt (until properly validated); (ii) filed for bankruptcy protection; (iii) is deceased; or (iv) provides necessary documentation showing he is the victim of identity theft.

## POLICIES AND PROCEDURES

Collections policies and procedures should be documented in detail and followed by all Members and their business partners.

These policies should include but are not limited to: account flow and work flow procedures, account handling procedures, payment handling and posting, work force training, quality assurance and monitoring, customer complaint handling, vendor or partner selection due diligence and monitoring, contract review and compliance, exception account handling (bankruptcy, consumer credit counseling services, dispute and fraud.

## **FAIR COLLECTION PRACTICES**

The Fair Debt Collection Practices Act (“FDCPA”) governs collection activities conducted by: (i) third party collection agencies collecting on behalf of Lenders; (ii) Lenders collecting their own debts suing an assumed name; and (iii) any collection agency that acquires the debt if the collector acquired the debt when it already was in default. The FDCPA contains a number of provisions that direct the manner in which a debt collector can contact a Consumer. Many states have adopted laws similar to the FDCPA; however, application of these laws may extend to the Lenders themselves when collecting on their own debt.

Even if a Member is not directly covered by the FDCPA or a similar state law, OLA believes that conformance with the Act’s requirements regarding interactions with Consumers constitute a best practice that OLA Members and any Agents or third parties with whom the Member does business should follow. Thus, we urge OLA Members to comply with the spirit of the FDCPA, even if not the letter of the law.

These Best Practices are as follows:

- Issue a written validation notice of the debt five days prior to making initial oral contact with each Consumer.
- Disclose the identity of the caller and state the purpose of the call.
- Ensure Mini Miranda is disclosed.
- Do not engage in false or misleading representations.
- Do not engage in customer harassment (an “excessive” number of calls) or abuse.
- Treat Consumers owing debts with professionalism, respect, and civility.

- Cease communication with Consumers where: (i) the account is disputed and until the debt has been appropriately validated; (ii) the debtor has filed for bankruptcy protection and has provided the proper documentation of such action; (iii) the debtor is deceased; or (iv) the debtor has provided the necessary documentation showing that he or she is the victim of identity theft.
- Comply with the Telephone Consumer Protection Act.
- Do not threaten to sue or criminally prosecute. Do not lead consumers to believe that they would be sued or subject to criminal prosecution if they did not make payments.
- Do not pressure consumers to pay off loan and quickly take out another one.
- Do not use legal jargon in calls to consumers, such as telling a consumer he could be subject to “immediate proceedings based on the law” if you do not actually sue consumers or attempt to bring criminal charges against them for non-payment of debts.
- Do not threatening to charge extra fees or report consumers to credit reporting agencies if that is not part of your corporate policy.

## **DISPUTE/FRAUD HANDLING**

In addition to establishing processes and practices relating to the collection of debts, Members and their Agents and other third party servicers must develop a process to investigate and handle disputes and to detect possible fraud. Accordingly, all

Loan servicers should adopt the following best practices:

- Validate Consumer information and receipt of funds from the original Loan.
- Report to proper authorities (i.e., local law enforcement) as needed.

## **GARNISHMENT OF WAGES**

Members must adhere to the following regarding garnishment of wages:

- Members shall not include, in any loan, loan contract, loan agreement or other document relating to a loan, any clause or other provision that constitutes or contains an assignment of wages or other earnings.

- Members and Vendors shall not disclose the fact of a borrower's debt to a borrower's employer, except with the borrower's consent or to effect a post-judicial remedy, such as to execute a valid court order for garnishment of wages.
- Members and Vendors should only contact an employer to obtain location information in accordance with FDCPA Section 804, and should never state to an employer that the borrower owes any debt.
- Members and Vendors shall not represent to a borrower or a borrower's employer that they have the right to garnish or otherwise receive a borrower's wages, except pursuant to a valid court order.
- Members and Vendors shall not represent that they are legally authorized or entitled to garnish wages of any individual under the Debt Collection Improvement Act of 1996, or any other state or federal law, without first obtaining a court order.

## **Repayment**

If a state has adopted a requirement for a repayment plan in state law, Members shall comply with those requirements.

If a customer is unable to repay the loan according to their original contract terms, members should create repayment plans (where not already mandated by state law) that provide flexibility based on the customer's circumstances.

## **Work Force Training**

Members shall create and maintain a comprehensive training plan and manual for employees. Training should include, but not be limited to the following:

- New hire training and manual
- Use of systems and tools
- Proper collections techniques and talk-offs (FDCPA compliant)
- Recurring training and modules
- Federal and State Laws and regulations (FDCPA, FCRA, TCPA, GLBA)

## **Quality Assurance**

Members shall create and maintain comprehensive quality and monitoring procedures. This should include, but not be limited to the following:

- Payment handling
- Account and work flow
- Customer Communication: (verbal, written, complaint handling)
- Debt Sales (see Collection Outsourcing and Debt Collecting in Vendor Selection)
- Third Party Contingency Collections (see Collection Outsourcing and Debt Collecting in Vendor Selection)

## **Bankruptcy Procedures**

All OLA members or partner companies who receive information regarding bankruptcy filings must:

- Develop a process to receive, update, and secure any information obtained relating to bankruptcy filings by customers.
- Cease all collections activities once bankruptcy information has been received or validated or the agency has reason to believe the consumer has filed for bankruptcy protection.

## **Dispute/Fraud Handling**

Members should develop a process to investigate and handle disputes and fraud accounts prior to continuing collection practices, which include: (i) validation of consumer's information and receipt of funds from original loan; and (ii) reporting to proper authorities as needed.

## **Customer Complaint Response and Tracking**

Members should develop and maintain a complaint management system to process, record and resolve complaints. This process should be consistent with any requirements imposed by a Member to respond to complaints submitted to the Consumer Financial Protection Bureau's complaint portal.

Member policies and procedures related to complaints should require the OLA Member to:

- Acknowledge all consumer complaints within the required timeframe and complete an investigation of the complaint.

- Resolve the problem in a manner consistent with company policy and OLA Best Practices.
- Keep the consumer and any agency involved informed throughout the process.
- Make sure the consumer viewpoint is given appropriate consideration in company decision making.
- Ensure appropriate resolution with consumer and any agency involved.
- Develop an action plan for complaint prevention.

### **Collection Requirements for Vendors**

Members who choose to outsource collection of outstanding debts should ensure they have a detailed process for choosing vendors; and which includes an ongoing monitoring process to ensure compliance with OLA Collection Best Practices and any applicable laws.

Before choosing a Vendor for collection activities, a Member should:

- Ensure the Vendor is licensed, bonded, and approved to collect in those states the lender plans to assign.
- Require compliance with all applicable laws and review Vendor's training, account review, call monitoring and customer complaint handling policy and procedures.
- Search for information from others in the industry regarding the Vendor and its business practices.
- Review association membership (*i.e.*, ACA, OLA, DBA, *etc.*) and management background.

All debt buyers who have purchased debt from any Member must follow all applicable guidelines, statutes and regulations as the Member.

# OLA Mobile Best Practices

## Background

As consumers are becoming increasingly comfortable with mobile applications, banks and other financial institutions are finding new ways to provide financial products. Despite the desire of both consumers and financial institutions to have instant access to credit, clear communication of disclosures and loan terms, data privacy and security remain important concerns.<sup>2</sup>

The FTC, in its February 2013 Staff Report, noted that mobile technology presents unique privacy concerns:

- **Personal Devices.** More than any other type of technology, mobile devices are typically personal to an individual, almost always on and with the user. This can facilitate unprecedented amounts of data collection, which could reveal sensitive information, such as communications with contacts, search queries and other highly personal information.
- **Facilitation of Data Sharing.** A single mobile device can facilitate data collection and sharing to a degree unprecedented in the desktop environment.
- **Information Location.** Mobile devices can reveal precise information about a user's location that could be used to build detailed profiles of consumer movements over time that were not anticipated by consumers.

In light of the unsettled legal environment, as well as the evolving nature of the technology involved, the OLA has developed these detailed Mobile Best Practices for all OLA Members to use in their businesses and for consideration by the CFPB when interpreting and enforcing the federal consumer protection law.<sup>3</sup>

For purposes of these best practices, "mobile financial services" ("MFS") refers to: mobile applications and mobile commerce. A "mobile device" includes smartphones and tablets but excludes

<sup>2</sup> Members must continue to adhere to the privacy and data security provisions contained in the OLA Best Practices. These Mobile Best Practices are a supplement to and are in addition to the requirements contained in that publication.

<sup>3</sup> Note that state laws may be more restrictive than as described in this document. For example, California's Attorney General recently announced that scores of mobile application developers are not in compliance with California privacy law because they are not conspicuously posting a privacy policy within the application. OLA Members should consult with local counsel about state law compliance.

laptops and other computers. A number of service providers will be involved in the deliverance of MFS. These service providers include Members who offer the MFS to customers and the developer that provides the platform for the MFS.

Unless stated otherwise, the Mobile Best Practices described herein apply to all entities involved in the utilization of mobile technology to market, originate and service small dollar loans. This includes Lenders, Vendors, Affiliates and any other third parties doing business with a Member.

By following these Mobile Best Practices, every Member will enhance its customers' experience and promote a positive reputation for the industry. These cohesive standards will ensure customers have a compliant, transparent and quality experience.

Additionally, we believe that these Mobile Best Practices will serve as strong guidelines for the CFPB and other regulatory agencies when ultimately determining compliance with existing consumer protection laws.

## **AUTHENTICATION AND SECURITY OF CONSUMER INFORMATION**

### **Authentication**

Members must authenticate every customer with whom they do business via an MFS. The method of authentication should be consistent with industry best practices and must identify the user as the Member's customer and further obtain authorization for the transaction.

The most common authentication method is something a person knows, commonly a password or PIN. If the customer types in the correct password or PIN, access is granted.

Nevertheless, because of the risk of fraud and identity theft, Members cannot rely on possession of the mobile device alone to permit access to the MFS.

If Members do not have mobile developers / mobile expertise in house to develop their own mobile solutions, they should utilize the services of a third party Vendor with domain mobile expertise. Specifically, Members should utilize vendors that provide software used to authenticate the customer via secure mobile authentication methods as well as capture customer information using encryption methods. Finally, Members must maintain any retained customer data in a secure environment.

## **Customer Security Measures**

Before engaging with consumers via an MFS, consumers should be advised to:

- Download the mobile application or access the mobile site from a reputable source, such as the Member's website or another credible source
- Keep password information safe and use strong passwords for all applications on their mobile device. Strong passwords consist of eight or more digits, with a combination of numbers and letters and capitalization.
- Never leave a mobile device unattended in a public place.
- Utilize the lock function on the mobile device and frequently change the lock password.
- Delete confidential information from the device prior to any third party servicing.
- Delete any financial information from the device.
- Discontinue use of the mobile banking application if the mobile device is stolen. Report the theft immediately to the Member.

## **Communications With Customers**

As an overarching policy, Members are advised that if they cannot articulate to users a reason why the Member is collecting the data, the Member should not collect it. Undisclosed data practices can get Members in trouble with the FTC and other regulators.

## **Utilize Mobile Technology Expertise**

To ensure that consumers will be able to view Members' communications, Members need to utilize technology designed to format the communication, content and functionality across ALL mobile devices. It is not sufficient to only maintain a website that a consumer may access via the Internet on his mobile device. Nor is it sufficient to maintain a "mobile friendly" site that does not consistently display and format information for every web enabled device that may be used to consummate a loan. Specifically, the Member needs to communicate to the consumer important information regarding loan terms and the privacy and security of his information. The Member cannot risk that the information as displayed on the consumer's mobile device is difficult or impossible to read because the documents contain small type, are truncated, cut off or contain margins that exceed the screen display. Attached to this document are

examples of documents that are not properly displayed via a mobile device.

Accordingly, Members without internal mobile developers and domain mobile expertise should utilize Vendor services that adapt communications with customers for mobile display. These solutions (either the Member's own or via a Vendor) should be able to identify the type of mobile device and operating system that the consumer is using to serve content specifically for the unique device. With this information the Member or Vendor can format loan agreements, disclosures and other important information in such a way that it will be legible by a consumer accessing the information via a mobile device. Consumers will not need to "pinch" the screen to manipulate the display to make the words more legible. A Member's reluctance to provide properly mobile optimized loan documents and disclosures likely will be deemed "misleading", "unfair" "deceptive" or "abusive" by a regulatory body such as the CFPB.

### **Obtain Consent To Communicate Electronically**

No Member may originate a loan until the consumer consents to receive disclosures electronically. To ensure this, Members must utilize an "I agree" or eSignature function to obtain this consent without which the transaction may not proceed further. This means that, unless the consumer consents to receive disclosures electronically by pushing the "I agree" or eSignature function required confirm button, the Member will terminate electronic communications with the consumer and will advise the consumer to contact a customer service representative. In addition, before the consumer binds himself to the mobile loan agreement, the consumer must indicate that he has the mobile capability to download and retain such disclosures received by email or text

To evidence compliance with this requirement the Member must either keep a copy of the electronic consent digitally signed by the consumer or be able to demonstrate that the transaction could not proceed further than the display of the consent request without the consumer's use of the "I agree" or signature function.

A sample consent that Members may utilize is attached.

## **Legal Requirements**

Communicating via MFS does not relieve the Member of its obligation to comply with all applicable federal laws governing those communications. Specifically, Members must continue to comply with the requirements that arise under the federal consumer protection laws. Accordingly, Members must ensure that they provide required disclosures consistent with any applicable requirements relating to format, font size, content, timing and manner of delivery (which requirements are typically set forth in the governing regulation) optimized for all mobile devices.

Thus, most consumer protection laws will permit a Member to provide information electronically, provided the Consumer consents to receive disclosures electronically and the Member otherwise communicates with the consumer in conformance with ESIGN. Below are some strategies that Members may employ to meet the disclosure requirements arising under federal consumer protection laws.

### **Gramm Leach Bliley Act – Privacy Notice and Opt Out**

Members must provide clear disclosures regarding their access, collection, use, storage and disclosure of personally identifiable information. Members must ensure that the full privacy notice is available to consumers; however, they may provide a “Short” Privacy Statement that is properly rendered for all mobile phones. The privacy notice should address key privacy concerns, such as what information is collected and with whom it is shared. This privacy notice should be clear, legible and tailored for display on all mobile devices.

If the Member will share the Consumer’s nonpublic financial information with non-affiliated parties, then the entity must give the Consumer the ability to opt out of that sharing. Consumers must receive this full privacy notice, before they receive any loan documents or other required disclosures to ensure that they understand what may happen to their customer data before they enter into a transaction with the Member.

Members also should ensure that all privacy policies address privacy protection in the mobile environment. This includes:

- Sharing data with third party advertisers for behavioral advertising purposes;
- Sharing data with third parties to allow other transaction data to be appended and used across sites;
- Accessing or sharing precise geo-location;

- Accessing photos and videos; and
- Accessing dialer or text messages.

Note that if Members are accessing geo-location information, Members should provide consumers with an opt-in consent (*i.e.*, gather such information only with affirmative consent from the consumer). As a general rule, Members should provide notice and consent for any data gathering and sharing practice that will “surprise” the consumer (such as accessing the consumer’s address book or photos).

Members also should adhere to any “Do Not Track” standards as created by the FTC that may apply to the mobile application environment (note that the FTC February 2013 report reemphasized the agency’s support of Do Not Track) as well as appropriate and applicable self-regulatory guidelines such as those created by the Digital Advertising Alliance (<http://www.aboutads.info>). These guidelines require that a company engaged in online behavioral targeting provide consumers with notice (in addition to its privacy policy) and an opt out choice with respect to the collection of his/her information and the use of that information in targeted advertisements.

### **Truth in Lending Act**

According to the federal Truth in Lending Act, all Members must disclose the appropriate information for the loan type originated (*i.e.*, closed-end disclosures for closed-end loans and open-end disclosures for open-end loans.). For closed-end loans, these disclosures include the Annual Percentage Rate, the Finance Charge, the Total of Payments, and the Payment Date and Amount. For open-end loans, different disclosure requirements apply.

For closed-end loans, the required disclosures must be grouped together and segregated from the loan agreement and terms. For open-end loans, the disclosures may be included as part of the loan agreement.

In either case (open- or closed-end) the disclosures must reflect the legal obligation of the Consumer. Said differently, the disclosure must accurately reflect the term, cost and repayment obligations to which the Consumer is bound. For example, if a Member requires repayment in one lump sum at a designated date, the disclosures must reflect that. In contrast, if a consumer agrees to an installment-based repayment plan, the disclosures must reflect that repayment plan.

The Member must provide these disclosures at or before the consumer becomes obligated on the loan, and these disclosures must be in writing and in a form that the consumer can easily read and navigate on the mobile device and ultimately retain (keep). Given the timing requirement, and the requirement that consumer receive the documents in a form that he can keep, Members will not be able to simply display the loan agreement with TILA disclosures electronically via a mobile device. Rather, the Member (on its own or *via* a Vendor) must also email a PDF of the loan agreement and disclosures to the consumer. The Member must ensure that the consumer is able to access these disclosures before he becomes bound to the loan agreement. The Member must obtain a proper mobile eSignature indicating acceptance of all disclosures prior to consummating the loan.

### **Additional Communications**

Upon receiving proper and explicit “opt in” permission, and with disclosure that data and message rates may apply, members may utilize text messaging to push useful information to the customer about the customer’s account, including:

- Technical support
- Alerts of deposit of funds into the customer’s account;
- Alerts of missed payments;
- Alerts of upcoming payment due date; and
- Alerts of servicing fees imposed, such as late or NSF fees.

Members also may provide information that may assist a struggling borrower, such as:

- Identification for financial counselors located in the customer’s geographic area; and
- Resources for customers who are suffering from financial strain.

Members who choose to engage in this type of communication should ensure that consumers are informed regarding their ability to opt out of receiving such communications as well as the steps that the consumer must take to opt out. Members should also be sensitive to the volume of messages sent to consumers and may want to provide consumers with a option to receive “fewer” or “more” communications from you.

Additionally, Members should adhere to the guidelines established by the Mobile Marketing Association (available here: <http://www.mmaglobal.com/node/2765>) when communicating via a mobile device. Mobile carriers will often require adherence to these guidelines and the failure to follow them could result in a carrier's blocking a Member's short code. Note that these guidelines apply to communications generally and are not triggered by advertisements.

## **Lead Generators**

If a Lead Generator is aware that a Consumer will interact with a Lender via a mobile application (*i.e.* a mobile lead), then the Lead Generator may not connect that mobile Consumer with Lenders who cannot provide mobile-enabled communications as described herein. Stated another way, Lead Generators should not present mobile leads to any lender who doesn't maintain a mobile optimized and compliant Mobile eSignature & Loan Disclosure process according to the OLA Mobile Best Practices.

## **Policies**

Every Member who plans to communicate with consumers via a mobile device should adopt a policy that conforms to all applicable laws and OLA's Best Practices. The policy should address, at a minimum:

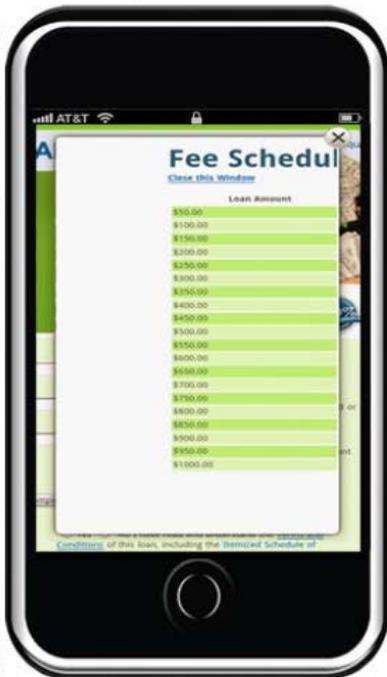
- Providing and receiving "stop" instructions to consumers. Any "stop" instructions should be provided to the consumer in BOLD lettering;
- Providing and receiving "help" instructions to consumers. Any "help" instructions should be provided to the consumer in BOLD lettering;
- Frequency of communications and the ability of the consumer to request a change to that frequency;
- Customer Service contact information (typically by providing a 1-800 number); and
- The fact that message and data rates may apply.

## Examples of Best Practices Violations

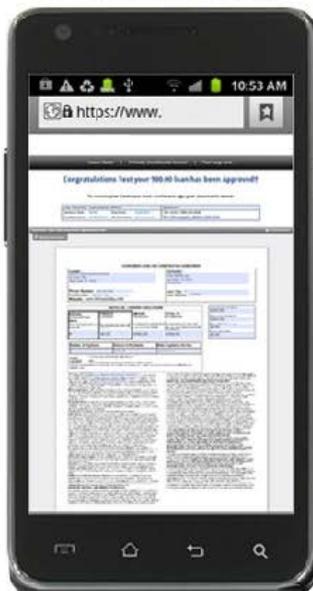
### Truncated terms



### Incomplete Content



### Font too small



### Mobile Security



## **ATTACHMENT "A"**

### **SAMPLE CONSENT TO ELECTRONIC DELIVERY OF DISCLOSURES**

By consenting to the electronic delivery of disclosures, you agree that we may provide electronically any and all communications regarding the loan application and the opening of the Loan (the "Disclosures"). This consent applies to the receipt of electronic Disclosures with respect to this loan application and the opening of the Loan. This consent does not apply to any future transactions that may occur between us.

#### **Paper Copies of Disclosures**

When you apply for and obtain a loan from [Lender], you may agree to receive information and disclosures regarding your loan electronically. You agree to print out, download or otherwise store the Disclosures and other communications to keep for your records. If you consent to the electronic delivery of Disclosures, you may also receive a paper copy of any Disclosure provided to you electronically by writing us at \_\_\_\_\_ . There is no fee for the paper copy.

#### **Withdrawing Consent to Electronic Delivery**

You may withdraw your consent by sending us your request in writing to: \_\_\_\_\_ . If you decide to withdraw Your Consent, the legal effectiveness, validity and/or enforceability of prior electronic Disclosures will not be affected.

#### **Hardware and Software Requirements to Print and Retain Loan Disclosures**

You must use a computer processor (CPU), monitor, modem with ISP access to the internet or direct-dial up accessibility and a printer capable of printing text screens or hard drive capable of storing data. In addition, you must use an internet browser software that supports 128-bit encryption.

If you want to review additional information on the requirements for using this software and associated hardware requirements, go to [www.microsoft.com](http://www.microsoft.com).

Because we may deliver Disclosures to you or otherwise communicate with you using e-mail, you must be able to send e-mail and receive e-mail that contains hyperlinks to websites.

## Procedures to Update Email Address

If you provide us with an email address in your application, you may notify us of changes in such address by writing us at \_\_\_\_\_.

## CONSENT AND ACKNOWLEDGEMENT

By clicking the "Sign Here" electronic delivery box below, or by signing below you acknowledge and agree that:

1. I have read the information about the use of electronic records to provide Disclosures and other communications, and the use of electronic signatures in connection with my loan application and Loan;
2. I consent to the use of electronic records to provide Disclosures and electronic signatures in connection with my loan application and Loan in place of written documents and handwritten signatures, when applicable.
3. I am able to view this consent. I am also able to download and review files on a mobile device.
4. I have an account with an internet service provider and I am able to send e-mail and receive e-mail with hyperlinks to websites.
5. I am consenting on behalf of all other co-applicants and co-owners of an account, if applicable. If applicable, I am authorized to consent on their behalf.

I acknowledge and agree that acceptance of this Notice and Consent Regarding Electronic Delivery of Disclosures inures to the benefit of \_\_\_\_\_, its affiliates, agents, employees, successors, and assigns.

\_\_\_\_\_  
Name

\_\_\_\_\_  
Date

## **ATTACHMENT “B”**

### **RESOURCES**

#### **Federal Trade Commission**

- February 2013 Staff Report: <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>
- Security Advice for Application Developers: <http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security>

#### **Workshop**

- <http://www.ftc.gov/bcp/workshops/mobilepayments/>

#### **Associations**

- Best Practices for Mobile Application Developers: <https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf>
- Digital Advertising Alliance: <http://www.aboutads.info>

#### **State Resources**

- California Attorney General; Privacy on the Go: [http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy\\_on\\_the\\_go.pdf](http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf)

## **ATTACHMENT “C”**

### **Glossary**

**Personally Identifiable Data.** Any data linked to a person or persistently linked to a mobile device: data that can identify a person via personal information or a device via a unique identifier. Included are user-entered data, as well as automatically collected data.

**Privacy Controls.** Settings available within an app or an operating system that allow users to make or revise choices offered in the general privacy policy about the collection of their personally identifiable data.

**Privacy Policy.** A comprehensive statement of a company’s or organization’s policies and practices related to an application, covering the accessing, collecting, using, disclosing, sharing and otherwise handling of personally identifiable data.

**Sensitive Information.** Is personally identifiable data about which users are likely to be concerned, such as precise geo-location; financial and medical information; passwords; and stored information such as contacts, photos and videos.

**Short Privacy Statement.** Is a privacy policy designed to be read on a mobile device, highlighting data practices that involve sensitive information or are likely to be unexpected because they involve data not required to an app’s basic functionality.

**Special Notice.** A timely, contextual notice that alerts users to a data practice that is likely to be unexpected because it involves sensitive information or data not required for an app’s basic functionality.

## **Vendor Selection and Compliance Best Practices**

The following types of businesses are intended to be covered by these Best Practices. Note that this list is illustrative in nature and is not meant to identify every type of third party which may offer services to a Member:

- Lead Generators
- Advertisers
- Payment processors
- Skip tracers
- Phone and letter vendors
- System or software providers
- Banks
- Call centers

### **CHOOSING A VENDOR**

Members should ensure that all marketing, collecting and processing practices conducted by third party Vendors on behalf of the Member comply with these Best Practices and applicable federal and state law, regulations, and guidelines. Accordingly, Members must monitor compliance with these Best Practices and applicable Laws and terminate relationships that fail to meet these Best Practices or comply with applicable laws. For example, this will require that Members take an active role in ensuring that Vendors such as Lead Generators adhere to the Best Practices described for advertising Loans, providing privacy policies and opt-outs from information sharing and protection of Consumer Information. If a Member does business with a Vendor that does not adhere to any Best Practice described here (with respect to the Member's business), the Member is deemed in violation of these Best Practices and the OLA Board may terminate that Member's membership.

To conduct an adequate due diligence of a Vendor, OLA Member should engage in the following activities (as appropriate for the relationship):

- Ask the Vendor to fill out a questionnaire that identifies key compliance issues – licenses, bonds, experience, staffing, complaints, outstanding litigation, audits, *etc.*
- Confirm that the Vendor holds current and appropriate licenses and bonds.

- Review the Vendor's policies, practices, training manuals, and scripting.
- Review the Vendor's websites and other consumer marketing materials.
- Review the Vendor's complaint handling procedures.
- Ask for references and recommendations.
- Confirm industry knowledge and experience of key professionals.
- Ask for professional accreditations and memberships.
- Require representations and warranties that the Vendor does business in compliance with all applicable laws. Seek indemnifications for breach of those representations.

## Appendix A – Definitions

**Advertiser** – A Member or its agent that generates online or offline Leads for short-term loans, via e-mail, search engine optimization, keyword buying, organic search, pay per click advertising, use of Affiliates, Direct mail DRTV, or any other method.

**Affiliate** – A person or entity that displays or distributes advertisements to drive traffic to a Member’s web site, or that collects Application information that it provides to a Member for further distribution through a Member’s network of Lenders.

**Agent** – One party acting on behalf of another, and binding that other party by words or actions.

**Application** – An online application form that collects personally identifiable information submitted by a consumer to a Member.

**Lender** – A lender offering short-term loans.

**Consumer** – A natural person who submits and Application for a short-term loan.

**Consumer Information** – Information that a consumer submits as part of an Application.

**Customer** – A natural person who has obtained a Loan.

**Lead** – A consumer interested in obtaining a short-term loan who has completed or partially completed an Application.

**Lead Generator** – An entity that procures Leads and offers them to Lenders. A Lender may act as a Lead Generator when it is unable to originate a Loan to a Consumer.

**Loan** – A short-term loan to a Consumer.

**Member** – A member of the OLA. Lenders and their Affiliates may be members of OLA

**Personally Identifiable Information** – Any information that may identify a Consumer by any characteristic, including, without limitation, the Consumer’s name, address, telephone number, e-mail address, bank or other financial account information, Social Security Number, date of birth and/or employment information.

**Sensitive Consumer Information** – Any sensitive Personally Identifiable Information collected from a Consumer including, without limitation, credit or debit card numbers, bank account information, Social Security Number, and date of birth.

**Vendor** – Any third party doing business with a Member.

## Appendix B -Federal Laws and Regulations

- **Electronic Fund Transfer Act/Regulation E.** This law protects consumers engaging in electronic fund transfers. Among other things, Regulation E Prohibits lenders from requiring, as a condition of loan approval, a Customer's authorization for loan repayment through an electronic funds transfer except in limited circumstances.
- **Equal Credit Opportunity Act/Regulation B.** This law sets forth requirements for accepting applications and providing notice of any adverse action and it prohibits discrimination against any borrower with respect to any aspect of a credit transaction on a prohibited basis.
- **Fair Credit Reporting Act.** This law requests that furnishers of information to consumer reporting agencies ensure the accuracy of data placed in the consumer reporting system. This law also prohibits the use of consumer reports for impermissible purposes and requires users of consumer reports to provide certain disclosures.
- **Fair Debt Collection Practices Act.** This law governs collection activities conducted by: (i) third party collection agencies collecting on behalf of lenders; (ii) lenders collecting their own debts suing an assumed name; and (iii) any collection agency that acquires the debt if the collector acquired the debt when it already was in default.
- **Gramm-Leach-Bliley.** This law prevents financial institutions from impermissibly sharing a consumer's nonpublic personal information with third parties, and requires that financial institutions disclose their privacy policies.
- **NACHA Operating Rules & Guidelines.** Provides users of the ACH Network with the legal framework for the Network.
- **Restore Online Shoppers' Confidence Act.** Federal law that prohibits online data passes and regulates the use of online negative option marketing.
- **Telephone Consumer Protection Act.** This law, along with Federal Communications Commission's implementing rules, regulates the actions of telemarketers and collection agencies.
- **Telemarketing Sales Rule.** These rules, enforced by the Federal Trade Commission, govern outbound and certain inbound telemarketing activities.

- **Truth in Lending Act/Regulation Z.** This law requires lenders to disclose loan terms and APRs. This law also requires lenders to provide advertising disclosures, credit payments properly and provide periodic statements.
- **Section 5 of the Federal Trade Commission Act / UDAAP.** Section 5 of the Federal Trade Commission Act generally prohibits unfair or deceptive marketing practices. UDAAP refers to acts or practices that are unfair, deceptive, or abusive.

**Deceptive.** An act or practice is deceptive when:

1. The representation, omission, act or practice misleads or is likely to mislead the consumer;
2. The consumer's interpretation of the representation, omission, act or practice is reasonable under the circumstances; and
3. The misleading representation, omission, act or practice is material.

**Unfair.** An act or practice is unfair when:

1. It causes or is likely to cause substantial injury to consumers;
2. The injury is not reasonably avoidable by consumers; and
3. The injury is not outweighed by countervailing benefits to consumers or to competition.

**Abusive.** An act or practice is abusive when:

1. It materially interferes with the ability of a consumer to understand a term or condition of a financial product or service; or
2. Take unreasonable advantage of: (a) a lack of understanding on the part of the consumer of the material risks, costs or condition of the product or service; (b) the inability of the consumer to protect its interests in selecting or using a consumer financial product or service; or (c) the reasonable reliance by the consumer on the lender to act in the interest of the consumer.

Consult with your legal counsel for other laws and regulations that affect your business.

# Appendix C -Validation of a Routing Number (2 methodologies)

## METHOD 1

The leading digits of a valid routing number are 01 to 12 OR 21 to 32. All others are leading digits are invalid.

Valid ABA's:

- 01254834
- 24643513

Invalid ABA's:

- 153218742
- 784318131

## METHOD 2

Validate the check digit.

An ABA is 8 digits, plus a 1 digit checksum as 9th position.

- Weighing factors (3, 7, 1, repeating). If the routing number is 07612324:
  - o Step 1 – Multiply each digit by weighing factor.
  - o Step 2 – Add the sums of all of the results (109).
  - o Step 3 – Subtract the sum from the next highest multiple of 10.
- Example if the sum is 109, the next highest is 110.  
Then subtract  $110 - 109 = 1$

|                 |   |    |   |   |    |   |   |   |     |
|-----------------|---|----|---|---|----|---|---|---|-----|
| 8 Digit ABA     | 0 | 7  | 6 | 1 | 2  | 3 | 2 | 4 |     |
| Weighing Factor | 3 | 7  | 1 | 3 | 7  | 1 | 3 | 7 |     |
| Sum             | 0 | 49 | 6 | 3 | 14 | 3 | 6 | 8 | 109 |

The check digit must equal 0 to 9 which is the last position of the routing number. Therefore the 9 digit ABA is: 076123241.

## Appendix D – Electronic Authorization Form

[Company Name]

I (we) hereby authorize \_\_\_\_\_, hereinafter called COMPANY, to initiate debit entries to my (our) \_\_\_\_\_ Checking Account/ \_\_\_\_\_ Savings Account (select one) indicated below at the depository financial institution named below, hereafter called DEPOSITORY, and to debit the same to such account.

I (we) hereby authorize COMPANY to debit \$ \_\_\_\_\_ on the:  
 1<sup>st</sup> of the month,  15<sup>th</sup> of the month, or  30<sup>th</sup> of the month  
(choose one).

I (we) acknowledge that the origination of transactions to my (our) account must comply with the provisions of U.S. law.

DEPOSITORY Information (Fill in below, or provide a voided check)

|                        |                         |
|------------------------|-------------------------|
| Depository Name: _____ | Branch: _____           |
| City: _____            | State: _____ Zip: _____ |
| Routing Number: _____  | Account Number: _____   |

This authorization is to remain in full force and effect until the COMPANY has received written notification from me (or either of us) of its termination in such time and in such manner as to afford COMPANY and DEPOSITORY a reasonable opportunity to act on it. Such notifications should be sent to: [ADDRESS/ CONTACT NAME/1-800 NUMBER].

## Appendix E – Vendor Agreement

### **THIRD PARTY COMPLIANCE WITH THE ONLINE LENDERS ALLIANCE BEST PRACTICES**

As a Member of the Online Lenders Alliance (OLA), you are required to comply with the OLA Best Practices (available at \_\_\_\_\_) and to ensure that any third parties with whom you do business to obtain or provide lead generation, advertising, marketing, customer service, and other such functions (collectively, “Vendors”), regardless of whether the Vendor is also a Member of the OLA, also comply with the Best Practice. Thus, in accordance with those requirements, the OLA provides the following language as an example of language that would be suitable for Members to include in their marketing and business agreement with Vendors:

“[Vendor Name] acknowledges that [Member Name] is a member of the Online Lenders Alliance and is obligated to comply with the Online Lenders Alliance Best Practices available at \_\_\_\_\_. Accordingly, in providing the services specified in this Agreement to [Member Name], [Vendor Name] represents and warrants that it will conduct its obligations and perform the services in compliance with those provisions of the Online Lenders Alliance Best Practices applicable to [Vendor’s] obligations under this Agreement, regardless of whether [Vendor Name] is also a member of the Online Lenders Alliance.”

The Best Practices are not intended to substitute for legal compliance and there may be other laws and regulations applicable to your business activities that are not covered in the Best Practices. Moreover, federal and state laws in this area change frequently. Members must continually monitor applicable laws, regulations, guidelines, and principles in consultation with capable counsel as necessary, to ensure that your business activities stay within the bounds of the law.

OLA is a self-policing organization. If OLA discovers or receives a report of any violations of the Best Practices, the OLA Board of Directors will take immediate action. The OLA Board will investigate the reported violations and will request and direct that the OLA Member address the issue immediately. The Board will monitor the Member to ensure future compliance. The Board has the authority to suspend and terminate membership if any Member is found to be in violation of any Best Practices.







