National Bureau of Business Licensing Officials
NBBLO

The Licensing Professional

Informing Licensing & Code Enforcement Officials

Vol. 17-1 Fall 2008

New Directions

By Paul Morris, ESQ & NBBLO Founder

We are pleased to announce that NBBLO is taking a new direction that we believe will significantly benefit all local government licensing officials who are involved with NBBLO. This change will lead to advances in NBBLO's responsiveness, its automation, its pledge to providing timely licensing educational services, and its commitment to moving forward the collaborative opportunity of licensing officials across the country.

We recognized that our expertise was in the substantive aspects of business licensing and not in webpage maintenance, blogging, listservs, electronic newsletters, etc. We explored options and realized that having an operative relationship with a company that has both an expertise in licensing and in automation was critical.

NBBLO has teamed up with Progressive Solutions, Inc. to provide all operations services for NBBLO. They have decades of experience in licensing and software and they understand what it takes to bring NBBLO to a 21st Century level. This will allow us to focus on what we do best in studying and reporting on the substance of business licensing.

(Continues on Pg 2)

In This Issue

New Directions

Continued from Page 1

This relationship will not affect the ability for other software vendors to participate and be involved in NBBLO's annual conferences. In fact, one of the reasons for this partnership is to enhance the opportunity for conference participants to see and learn more about the services available to assist in improved licensing. Conference attendees at our Silver Anniversary 25th Annual Conference in Atlanta will see a much better exhibitors area than we have ever had.

Our webpage, www.nbblo.org, has already been improved and stay tuned for more upgrades and enhanced services in the coming weeks. We are excited about this relationship and its advantage to you, the members of NBBLO!

Planning for Successful Revenue Collection

By David McPherson, Deputy Finance Director, City of San Jose

The City of San José recognized the need to improve revenue collections. So the City implemented the Revenue Collection Strategic Plan (RCSP) which increased collections and improved the collection processes.

The goal of the RCSP was to implement an aggressive revenue collection campaign intended to develop targets and provide assessments as to how staff were spending their time. The RCSP commenced in January 2007 with the restructure of operations to maximize the effectiveness of the Investigator Collectors' time spent on collections.

The first part of the plan was to develop methods that would improve morale and working conditions. In order to figure out how to accomplish this, a survey was completed by staff to find out what their needs were. As part of this analysis we identified that most employees did not have the proper tools to do their job, had limited technological support, lacked job growth opportunities and time to do revenue collections. Furthermore, most of them did not have defined goals and targets for their jobs.

Therefore, specific targets were adopted which included increasing the Business Tax revenue base, reducing the average number of days accounts remained past due, auditing programs which generate revenue (i.e. Transient Occupancy Tax, Utility User Tax, and Sales Tax) and improving customer service. A theme of "Show Me The Money" was incorporated to remind staff of what their priorities were without giving up quality customer service. Staff was encouraged

News & Notes

» At the California Municipal Tax & Revenue Association in October 2008, Paul Morris presented an update of case law and Glenn Vodhanel presented a revised seminar on "Automation and Efficiency for Business Licensing."

» The 2009 conference will be held in Atlanta, GA from July 15-17, 2009. For details see page 8 or go to www.nbblo.org and click on Conferences.

Downtown Bill Wooten

to come up with innovative ideas, think outside the box and to take risks in creating new streamlining ideas.

Prior to the RSCP, time allocation for collections was at 28%, customer service 26%, support services 24% and other non collection functions made up the remainder 22%. With implementation of the new program, the goal for collections was 70% and for all other functions 30%.

A Pilot Program was developed to test the second part of the plan, and this part was to demonstrate the need for support staff to alleviate the non-collection duties the Investigator Collectors were doing. During the six month Pilot Program the RCSP generated $5.2 million dollars with an ROI of $16.76 compared to entire previous year's collections of $2.1 million dollars with a ROI of $4.81. Another benefit of the RCSP was a reduction in response time to customers' inquiries by 40%.

As a result of the success of this Pilot Program the Finance Department was able to retain the additional support staff as permanent employees. The program has continued to prove its value by generating $10.8 million dollars or a 408% increase over its target for the 2007-2008 fiscal year.

In summary, it is important to note that if an organization is unclear about its purpose or has been given multiple and conflicting purposes it cannot achieve high performance. It is imperative to create a focused vision where staff can actively participate in the outcome which allows them to help develop, take ownership and pride in the plan and will ultimately result in them "Showing you the Money."

Ten Common Mistakes in Responding to a Data Breach Incident

By Reece Hirsch

One year after the ChoicePoint incident cast a spotlight on security breach notification issues, a few lessons have been learned by businesses responding to, or seeking to avoid, data breach incidents. Some of these lessons have been learned the hard way by companies that have experienced negative publicity, state attorney general and Federal Trade Commission scrutiny, declining stock prices, and class action lawsuits.

As the saying goes, those who do not learn from history are doomed to repeat it. This article outlines ten common mistakes to avoid in responding to data breach incidents.

1. Overreacting. Once a company has sent a security breach notice to its custom-

Code Enforcement Officer Killed

On Thursday, November 13th 2008, code enforcement officer Rodney Morales, 40, was shot while investigating a routine zoning complaint in Aurora, Colorado.

He was taken to a local hospital where he was pronounced dead about an hour later.

Police are searching for the killer and have indicated there is a $10,000 reward for information leading to the shooter's arrest and conviction.

Our hearts go out to the family of our fallen code enforcement brother.

ers, it is impossible to "un-ring the bell." On the other hand, statutes such as California's S.B. 1386 require notification "in the most expedient time possible and without unreasonable delay." These two competing imperatives may be balanced only if a company is prepared to conduct a thorough investigation of a potential data breach immediately upon becoming aware of an incident.

For example, one client company learned that a laptop containing a wealth of confidential customer data was missing. The company commenced preparations to notify its customers around the country. At the same time, the company launched a vigorous internal investigation that included questioning of a security guard who had access to the laptop. The security guard soon confessed that he had hidden the missing laptop within the company's offices with the intention of removing it later. The company had no reason to believe that the laptop had ever left the premises or that the data had been accessed by an unauthorized person. The company was fortunate because it was able to bring its investigation to a prompt and successful conclusion before sending more than a million notice letters to customers.

2. Failing to Adopt a Security Compliance Program, Including an Incident Response Plan. In the past few years the framework of data security laws, regulations, and industry standards has evolved, and now includes state security breach notification laws, the Payment Card Industry (PCI) Data Standard, the Gramm-Leach-Bliley Act safeguards rules, the FTC's regulation of security practices under the "unfairness" doctrine, California's "reasonable security procedures and practices" law (A.B. 1950), the federal bank regulatory agencies' guidance on consumer data breaches, and the Health Insurance Portability and Accountability Act (HIPAA) security rule. As a prudent risk management practice and to comply with these new legal and industry standards, it is important for companies to conduct a formal information security risk assessment and adopt written policies and procedures based upon the findings of that assessment. A data breach incident response plan is an integral part of any comprehensive security compliance program.

As noted above, state security breach notification laws generally require notices to be sent very promptly. In a guidance document, the California Office for Privacy Protection recommended that notices be sent within ten business days. In order to respond in such an expedited manner, particularly given the complex logistics of printing and mailing a mass notification, it is vital to have an incident response plan. Precious days can be lost if a company is forced to formulate its approach on the fly.

3. Failing to Follow an Incident Response Plan. In the heat of a crisis, companies sometimes neglect to follow the security incident response plan that they have adopted. If a company's response to a data breach incident later comes under scrutiny by regulators or the plaintiffs in a class action lawsuit, the company generally will be well-served if it can demonstrate that its response was reasonable. The easiest way to demonstrate that a company failed to act reasonably is to show that it adopted prudent, industry-standard security incident response policies and procedures—and then failed to follow them.

4. Not Training Your Personnel to Spot Data Breaches. To many within an organization, the theft of a laptop may not seem like a major event. However, if that laptop contains the Social Security numbers of all of a company's customers, the theft, if not properly handled, could have a catastrophic impact

on the future of the company. One of the most important aspects of a security compliance program is educating employees so that they can identify and promptly report to their supervisors potential data breach incidents.

One of the worst situations to be faced with under state security breach notification laws is learning of an incident too late. Occasionally, an employee will report an incident, such as the theft of a laptop containing personal information, to their immediate supervisor. If the employee and supervisor are not sensitized to data breach issues, weeks may pass before the privacy officer or management become aware that a potential data breach has occurred. At that point, the company is faced with the unpleasant prospect of being legally required to report to its customers an incident in which the company has clearly failed to comply with the applicable security breach notification law.

5. Failing to Follow Forensic Procedures. For breaches that involve identity thieves or other wrongdoers, the ideal outcome is the apprehension of the perpetrator and the recovery of the data before customers are harmed. Failure to follow proper computer forensic procedures may erase or spoil the evidence that could lead to prosecution or apprehension of such criminals. Companies should identify internal or external computer forensic resources in advance so that they can be mobilized quickly when a breach occurs. If the company intends to utilize external forensic consultants, internal IT staff should receive training regarding proper coordination with the consultants and avoiding destruction and contamination of evidence.

For example, by starting an investigation and reviewing the systems directly without first making a forensic image, you risk changing the "access" and "modified" dates (both a form of metadata) of the relevant files. Once you do that, you can't prove when they were last accessed or modified, and can't match the forensic image up with logs that may show a hacker's IP address. By first making a forensic image, you preserve everything—including the metadata—so you can return to that "snapshot" at any time.

6. Inadequate Management of Vendor Relationships. California's S.B. 1386 requires that any person or business that maintains computerized data that includes personal information that it does not own must notify the owner or licensee of the information immediately upon learning of a security breach. A company that entrusts its customer information to third party vendors should make sure the vendors understand this legal obligation. It is also advisable to require the vendor to notify the company of the breach within a specified time frame (i.e., 24 hours or 2 business days). In certain cases, it may also be prudent to specify in the vendor agreement a process for coordinating with respect to breach notification and the content of the notice letter.

7. Failing to Coordinate Effectively With Credit Reporting Agencies. When a security breach incident occurs, the company should consider notifying credit reporting agencies before sending a notice to customers. If a police report has been filed, customers may find it useful to receive a copy of that report along with the breach notification. Having a copy of the police report in hand may make it easier for customers to reference the incident when communicating with credit reporting agencies. Companies should also consider offering free credit reporting for a specified period (i.e., one year) to affected customers.

8. Failing to Coordinate Effectively With Law Enforcement Authorities. S.B. 1386 and most other state security breach notification laws provide that notification may be delayed if a law enforcement agency determines that notification will

impede a criminal investigation. A company should not delay notifying customers based upon such provisions unless they receive strong confirmation, preferably in writing, from the relevant law enforcement agency that the notice would impede the investigation.

A company should carefully consider the appropriateness of notifying law enforcement of an incident, as well as which agency might most aggressively pursue the case. A routine laptop theft may or may not receive prolonged attention from the local police department. However, if the breach is the work of a sophisticated ring of hackers, then the case might be attractive to the local high tech crimes task force, the FBI, the Secret Service, or the National Infrastructure Protection Center.

9. Forgetting That State Security Breach Notification Laws Differ. California's S.B. 1386 was the first security breach notification statute and it remains a model for many other state laws. However, some security breach notification laws differ from S.B. 1386 in significant respects. For example, under the security breach notifications laws of certain states (such as New Jersey, New York and North Carolina) specified state agencies must be notified of the breach, in addition to the consumer. Other states (including Georgia, Maine, Minnesota, Montana and Nevada) require notification of credit reporting agencies. A company experiencing a security breach should review the security breach notification laws of all states in which personal information has been compromised and formulate an incident response that complies with all applicable notification laws.

10. Lawyers and IT Personnel Must Speak a Common Language. Terms such as "breach" and "access" can have very different meanings when spoken by lawyers, IT personnel, and company executives. Developing an incident response team in advance allows the participants to make sure they are speaking a common language before the bullets begin flying. For example, a phishing scheme might be loosely referred to as a breach, when it actually does not constitute a breach triggering notice under state security breach notification laws. A typical phishing scheme does not involve the unauthorized acquisition of data maintained by the company. Instead, it usually involves the use of deception to obtain a user ID and password from the customer. A security incident response team should bring to bear, in a coordinated fashion, all of the skills needed to effectively respond to a data breach crisis, which may include personnel from legal, information technology, management, compliance, public relations, investor relations, and human resources.

Reece Hirsch, a partner in the San Francisco office of Sonnenschein Nath & Rosenthal LLP, specializes in privacy and data security issues. He can be reached at (415) 882-5040 or rhirsch@sonnenschein.com.

Review of 2008 Conference in Denver, CO

The 23rd NBBLO conference was held in Denver this past July, 2008.

Speakers presented topics on case law, revenue enhancement and efficiency via automation.

77 Representatives of jurisdictions from 19 States came together for an informative and substantive discussion of issues important to state and local government licensing and code enforcement officials.

2003 Flashback: Nevada Secretary of State Steps Up Late Fees

In a policy that may be the first of its type in the nation, Nevada Legislature via NRS 225.085 as approved June 9th of 2003 required Secretary of State filings to be placed in the care, custody and control of the Secretary of State. Subsequently, the Nevada Secretary of State per NRS 225.85.3 no longer accepts USPS postmarks as evidence of timely filing. These Secretary of State policies require that Secretary of State filings must be complete with payment in full and acknowledged as being in the possession of the department before the deadline or any tendered payment will be deposited and the filing returned for additional fines and penalties. While staff members may process payments on the date received, it is conceivable that payments submitted via mail on or prior to the due date may well increase late fee and penalty revenue. While Federal Treasury regulation 301.70502-1 currently does not follow this policy, I can only imagine the penalties/ late fees to be generated by the Federal Government should they enact a similar policy not to mention the potential taxpayer revolt that would likely accompany it.

2008 Update: The outrage from the 2008 Banking Bailout Bill could seem miniscule in comparison should any similar modification to Federal timely filing rules be attempted.

Wise quotation: *You can only govern a population about as much as they let you!*

The ABC's of Electronic Payment Processing

By: Glenn R. Vodhanel, CEO of Progressive Solutions Inc.

In days not so long ago, only acronym ACH was commonly known and then only to those in utility divisions who regularly accepted recurring payments.

Today there is an entire alphabet soup of additional acronyms and terms related to electronic payment processing. This article is intended to present a glossary of terms used in establishing an electronic payment processing system and at the same time address other important issues that may not be commonly known.

Remember-- the only person who should be presenting a credit card is the person whose name and signature are on the credit card. Should you accept such a transaction be forewarned as frequently the card holder will receive their statement and dispute the charge. Should you desire to accept a transaction from someone who is not physically present, contact the card holder and request a fax which identifies all card info plus the amount authorized, the billing address of the card and the authorizing signature.

ACH: Automated Clearing House. An electronic network for financial transactions in the US which is used to clear (process) electronic check transactions.

ARC: Accounts Receivable Conversion (Used to convert physical checks received by mail to electronic payments)

Authorization: the process where a check is submitted (via the internet) by the municipality (or retailer) for authorization by the merchant account provider. No transaction is finalized until settlement.

AVS: Address Verification Service used to electronically authenticate credit cards with the cardholder billing address.

Card Not Present: Credit Card payments that occur without face to face contact with the cardholder such as: Mail, Telephone, Fax and the internet. (Generally you may not accept card not present transactions unless such authorization is provided within your merchant agreement.)

Card Present: Over the Counter Transactions where the credit card is physically present and generally swiped.

Cash Discounts: Are allowed in the context of most merchant agreements.

Consolidated Account Processing: The concept where a citizen upon visiting a payment window with his address, name or consolidation id may identify all outstanding receivables to facilitate payment of balances due. PSI's OneStop™ product incorporates this functionality. The various options relating to the mechanics of this process will be detailed in a subsequent article.

CVV2/CVC2: Card Authentication Value 2 uses a 3 digit number printed on the credit card to authenticate the payment transaction.

BOC: Back Office Conversion. Acceptance of a physical check over the counter and conversion of the check to a digital transmission behind the scenes or in the back office.

Chargeback: Whenever a customer disputes/questions a transaction that has been deposited into your account, the merchant account provider will debit your account in the amount of the transaction until the customer issue is resolved. In addition to the above debit, your account may be subject to a $50 chargeback fee if you fail to follow card acceptance and authorization procedures.

EBPP: Electronic Bill Presentment and Payment facilitates cost effective transmission of bills via email and/or printed media and optionally also facilitates customer payments over the counter, via IVR and the internet.

E-Check: entry of checking account information with which to process a payment via electronic check.

ESIGN: Electronic Signatures in Global and National Commerce Act enacted by Congress June 30, 2000 to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

Frank: To mark a check as scanned by printing information on one side of the check.

Gateway: 3rd party vendor that funnels credit card information to the credit card holder's bank for validation and returns authorization information. A gateway provider is often utilized so a software vendor may focus effort on enhancing their software rather than expending time jumping through the hoops of each potential banking partner.

Interchange Fees: The percentage charged by the merchant account provider to process a credit card transaction.

IVR: Interactive Voice Response. Customers interact via telephone with a computer to retrieve balances, documents and may even accept payment of outstanding city receivables. Voice recognition is commonly an option. Payments may flow directly to a central cashiering system such as Ca$hierCentral.

Lockbox: A service, often provided by a banking institution, in which payments are processed by the bank and each transaction is transmitted to the customer via an electronic file for input into and update of their receivable system(s).

Merchant Account: A specific type of banking account which is created for the purposes of accepting credit card payments. A merchant account agreement is required which sets forth the requirements and the fees associated with the account (Especially Interchange Fees).

NACHA: National Automated Clearing House Association. A standards board that has established the defacto standard for electronic payment transmission in the US.

Notification: Prior to truncation (conversion of a payment by check to an electronic format), the customer must receive proper notification per the terms of your merchant agreement.

Pilot Program: A program intended to enable municipalities to charge a percentage based surcharge for the convenience of using a credit card to pay consumer tax payments. Only available to registered merchants who demonstrate PCIDSS compliance.

PCIDSS: Payment Card Industry Data Security Standards

Privacy: Listing cardholder's personal information on a credit card draft such as expiration date and full credit card number may be prohibited by both state and federal law.

RDC: Remote Deposit Capture. Both sides of the check are digitally scanned and transmitted/deposited along with the bank account number and amount paid in lieu of the physical check.

Rebuttal: A merchant's written response to a chargeback that documents the validity of a transaction and that proper procedures were followed. Rebuttals must be completed within the number of days indicated on the chargeback notice.

Recurring Payment: An arrangement initiated by a customer which authorizes payment via the specified method at a predetermined interval for the bill amount. (i.e. ACH, Debit or Credit Card)

Retention: Many merchant account providers require retention of signed sales drafts for 18 months.

Returned Item: ACH, ARC, BOC and checks rejected because they are unable to be processed.

Sales Returns: Any condition(s) that limits the cardholder's ability to return merchandise must be clearly stated in bold print in letters .25 inches high near the cardholder signature on the sales draft or order form for mail order.

Settlement: The time each day when a credit card transaction is finalized (often 11pm).

SSL: Secured Socket Layer enables industry standard secured payment processing via data encryption.

Surcharges: Encouraging patronage, prompt payment of bills and not penalizing customers for paying with a credit card makes good business sense as it saves all effort associated with the paper flow and possible bad checks associated with non credit card transactions. Adding a surcharge to over the counter credit transactions is against the law in many states and violates many merchant account agreements. It may be allowed for government or schools for utilization of alternative payment modes such as telephone and internet.

Truncation: Checks less than $10,000 may be converted to a simplified all digital transaction which does not transmit check images.

Payment Processing Cost Considerations

By: Glenn R. Vodhanel, CEO of Progressive Solutions Inc.

Old fashion ways of transacting business are too costly and labor intensive given the automation opportunities available today. Furthermore, failure to accept credit cards dramatically diminishes your revenue potential. This article is intended to clearly illustrate the benefits versus the drawbacks and to promote efficiency via automation!

Given today's business environment, what is the common customer expectation? Acceptance of credit cards, cash and checks *(without a discount promoting one method of tender over another and without assessing a surcharge)*.

Surcharges tend to reduce the quantity of payments and leave customers feeling nickeled and dimed. Previously, many banks charged for each ATM withdrawal. Customer dissatisfaction resulted in opportunities for customers to avoid fees which they took advantage of in droves.

In our economic situation, if a payer does not have cash for a business license, utility bill or other municipal obligation and your municipality does not accept credit cards, you will very likely not receive payment. However, if you do accept credit cards and the payer is not at their credit card limit, you are much more likely to receive payment and the burden of collecting such funds then falls to the credit card issuer. In a nutshell you will have plugged into a revenue source previously untapped by your organization.

Unfortunately, governmental entities often tend to focus on the missing piece of the pie rather than the extra pie that becomes available as a result of embracing revenue enhancement efficiencies such as credit card processing or other more efficient means of payment such as electronic bank transfers.

It is true minimal transaction costs are associated with credit card processing. However, these costs are best evaluated by considering the reduction in staff costs required to process

Benefits	Drawback
Increased revenue as a direct result of credit card acceptance. Receivables will drop.	An approximate cost ≤ 2%
Reduced labor/costs so staff time may be reallocated to more productive endeavors (such as revenue enhancement activities)	
Business Friendliness (Make it easier for customers to tender payment in the correct amounts 24/7 from anywhere in the world via internet and Interactive Voice Response-telephone payments)	
Save your customers gas, time and help the environment (carbon emission reduction is eco-friendly)	
Enable the disabled to pay their bills without physical hindrance. (Another accommodation for the disabled)	
Reduce paper flow (Use email notification. Save a tree and postage)	
Eliminate unnecessary processing of paper based payment transactions (additional phone & counter staff, mail opening, bank deposits, accounting, bank reconciliation & the potential for misplaced checks).	
Reduce confrontations and stress dealing with disgruntled citizens who feel they are already paying more than their fair share.	
Costs may be managed and maximum benefit achieved by limiting credit card transaction amounts (i.e. a maximum of $5,000 per transaction).	

paper based transactions. Generally, overall automated transaction costs will be cheaper and offer the opportunity to dramatically reduce paper based transaction costs.

Given the additional revenue available from credit card processing, *would you rather refuse additional revenue* by not accepting credit cards *or increase revenue* and pocket 97% of the additional revenue generated? To really fire up revenue collection, redirect the staff time that is freed up toward other revenue enhancement activities. With proper direction, success is inevitable!

Glenn Vodhanel, CEO of Progressive Solutions Inc., has over 30 years experience in the government sector and often consults and speaks rendering expert advice on efficiency via automation.

He may be contacted at: glennv@progressivesolutions.com

Exhibitors at the Denver Conference:

Company	Representative	Telephone
Progressive Solutions	Chris Retzinger	(714) 671 - 1597
HDL Companies	Marta Bonin	(909) 861 - 4335
MuniServices	Patrick Scott	(559) 271 - 6811
Tax Compliance, Inc	Arianne Turnier	(858) 547 - 4100 x351

2010 Conference Proposals Requested:

Proposals are currently being accepted from all cities desiring to host the 2010 NBBLO Conference to be held July 14th-16th. Please send a designated host city contact and proposed host hotel contact information to confmgr@nbblo.org

Upcoming Events:

Association Name	Conference	Website
Florida Association Code Enforcement	June 16-20, 2009	www.face-online.org
Alabama Municipal Revenue Officers Association	July 8-10, 2009	http://www.amroa.org
National Bureau of Business Licensing Officials	July 15-17, 2009	www.nbblo.org
SC Business Licensing Officials Association	September 2009	www.masc.sc/affiliates/bloa/description.htm
Code Officials Association of Alabama	September 2009	www.coaa.com
California Municipal Revenue & Tax Association	October 2009	www.cmrta.org
California Association of Code Enforcement Officers	October 2009	www.caceo.us

Sign up for the July 2009 Conference in Atlanta, GA

Sign up for the 25th Annual State and Local Business Licensing Conference to be held July 15-17, 2009 in Atlanta, GA

Just go to www.nbblo.org and click on “Conferences” and then “Conference Registration.” There you can fill out the form online and submit it. Thereafter, you send the appropriate fee to the address shown. Or you can just call 801-261-8266 and register by phone.

There is an outstanding conference agenda. Come hear discussions of regulatory licensing issues as well as issues germane to tax collection. Local business licensing is a unique specialty and it’s difficult to find resources applicable to your needs.

What is particularly helpful, is associating with your peers from across the country who have similar issues that you are confronting.

In addition to the substantive material there is a great opportunity to see and experience Atlanta in all of its beauty and historical grandeur.

See you in Atlanta GA!

National Bureau of Business Licensing Officials

NBBLO, LLC
PO BOX 67
New Creek, WV 26743

Website: www.nbblo.org
Phone: 801-261-8266
Fax: 801-415-9472
E-mail us at:
confmgr@nbblo.org
editor@nbblo.org

Informing Licensing & Code Enforcement Officials

Becoming a Member

NBBLO membership enables you access to information regarding code enforcement, regulatory and revenue raising business licensing at the local level of government.

Membership is only $45 annually and entitles you to a discounted annual conference registration and two newsletters a year. NBBLO also sponsors several national certifications.

For more information go to www.nbblo.org. There are links for membership, certification, and the annual conference. Our next conference will be in Atlanta, GA, July 15-17, 2009 at the Atlanta Marriott Marquis.

Membership Fees:

$45 Early
$55 Late (After February 28)

Article Contributions & Permission to Publish:

This publication is the result of a collective knowledge developed and refined over many years. We greatly appreciate words from our readers; please, share your knowledge and stories.

By submitting an article for publication, author agrees to share their copyright with NBBLO, LLC for any article accepted and published. The NBBLO reserves the right to edit any article as deemed necessary at our sole discretion.

Please direct your ideas, articles, and requests for permission to republish articles to: editor@nbblo.org