MAILING COMPLIANCE BEST PRACTICES: WHAT EVERY BUSINESS NEEDS TO KNOW

For more information please vist:
http://www.pb.com/equipment/

Pitney Bowes

CONTENTS

IS YOUR MAILING OPERATION COMPLIANT?

For many mailers, the answer is a hesitant "maybe". The reason for this is simple: staying compliant with the complex laws that surround mailing in publicly traded companies and regulated sectors is a big challenge. And the fact that these laws vary from industry to industry and from state to state further adds to the difficulty.

Unfortunately, the penalties for non-compliant mailing practices are significant, and most organizations are not even aware that they are at risk. To put it into perspective, printed data is subject to many of the same regulations as electronic data and, while almost every business now goes to great lengths to protect their electronic communications, very few have the comparable safeguards when it comes to their printed mail.

To assist businesses that want to bring their mailing operations into compliance, Pitney Bowes has created this resource to highlight the key regulations that may impact mailing operations, along with best practices that will help to reduce risks and make mass mailings more efficient.

1.0 REGULATIONS THAT IMPACT MAILERS

A number of privacy and security regulations can affect mailing operations. Below are four of the most important regulations, as well as the consequences for those found to be in violation of them:

1.1 Sarbanes-Oxley

The Sarbanes-Oxley (SOX) Act of 2002 was enacted in response to the high-profile financial scams that have cost investors billions of dollars. The legislation aims to protect the public and investors from fraud. Compliance with SOX is mandatory for all publicly traded companies. Private companies that are planning for IPOs should also prepare for compliance.

The effects of SOX on an organization can be widespread. If a publically traded company relies on postal mail for marketing or day-to-day operations and the same is material to its financial condition, it may be required to accurately track postage and shipping expenses in order to meet SOX requirements. However, ensuring accuracy can be difficult – especially for large organizations that mail from multiple locations and don't have a standardized reporting process for all offices and departments.

Consequences

Failure to comply with SOX regulations means that senior management can be held criminally and civilly liable for inaccurate reporting. Organizations may also face a public relations crisis that undermines stock value.

1.2 Gramm–Leach–Bliley Act

The Gramm–Leach–Bliley Act (GLBA) affects organizations in the financial sector and is designed to secure the privacy of consumer financial data.

Although financial institutions spend a lot of time and resources encrypting their electronic information, they often don't put the same effort into protecting their

printed mail. Financial institutions outsourcing their mail handling can find it hard to ensure the accuracy and security of every consumer notice and statement. They may also lack an audit trail that traces each mail piece through the postal system. If consumer data in postal mail falls into the wrong hands, an organization may be held accountable for a GLBA violation.

Therefore, the best way to handle these communications is by engaging in "best practices." For example, if a financial institution is using a third-party for its mailings, it can ensure its supplier meets "standard certification requirements" for mailing and data security. If a financial institution is processing its mail in house, there are insourcing technologies that can help them with security, such as "file based processing" that provides proof-of-content and proof-of-production for each individual mailpiece. In addition, Intelligent Mail barcode technology (in IMb tracing, such as TrackMyMail™) can ensure and provide proof-of-mailing verifications.

Consequences

Any business caught in violation of GLBA faces a penalty of $10,000 per incident plus an automatic audit by the Federal Trade Commission for the next seven years. The same company will also need to perform public self-admonishment, such as taking out an ad in the paper acknowledging guilt of a violation.

1.3 Health Insurance Portability and Accountability Act 2.0

The Health Insurance Portability and Accountability Act (HIPAA) 2.0 impacts healthcare organizations and protects patient and consumer privacy. HIPAA regulations are even stricter than GLBA regulations because they specify that only authorized employees can view patient information.

Like other industries, many medical practitioners have gone to great lengths to safeguard their electronic data, but they often don't have as much control over their postal mailings. When mail preparation is outsourced, the people who handle patients' medical claims

forms, statements, and other sensitive information may not be authorized to do so. This increases the likelihood of security breaches and the theft of personal information, such as Social Security numbers. In order to minimize this risk, medical providers should engage in "best practices" and ensure that third-party suppliers meet standard certification requirements.

Insourcing technologies can also monitor the processing and paper-handling events to ensure that only authorized personnel are performing the mailings and in contact with the mailings at the facility where mail is produced. "File based processing" technology further provides proof-of-content and proof-of production of each individual mailpiece in-house. And Intelligent Mail barcode technology (in IMb tracing, such as TrackMyMail™) can ensure and provide proof-of-mailing security.

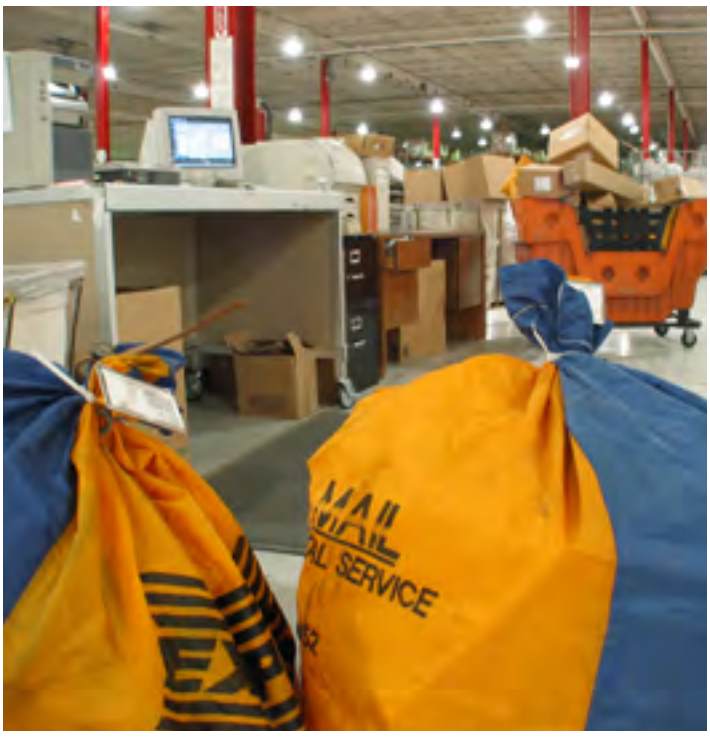
Consequences

In 2009, HIPAA 2.0 initiated tougher penalties for violations. Fines range from $25,000 to $1.25 million, depending on the severity and frequency of the offense.

1.4 State Insurance Regulations

State insurance regulations affect insurance providers who mail non-renewal or cancellation notices to the insured. Nearly every state requires proof that the insurance provider mailed the notice within a certain period of time. This "proof of mailing" only requires the insurer to prove that it mailed the notice, not that it was received. What many mailers don't realize is that USPS does not offer a named "proof- of- mailing" service, resulting in too many mailers failing to select the optimal service.

Pitney Bowes can offer postal induction evidencing technologies, such as TrackMyMail™, to validate these occurrences.



Consequences

Organizations may face legal consequences if the insured files a claim and it can't be proven that a notice was mailed. Should an organization deny the claim, the insured can take the case to court and sue for damages. In the absence of proof of mailing, the organization may lose the case.

2.0 THE RISKS OF OUTSOURCING YOUR MAIL PREPARATION

Organizations relying on postal mail for their operations, marketing or customer service face a number of risks when they outsource their mailings to a third party, including:

- Poor visibility. Although USPS offers the technology for tracing mail, most fulfillment houses do not. This means sensitive information may disappear into a black hole where it is impossible to track any given piece at any given time.

- Lack of quality assurance. Some third-party mailers can't provide evidence that a mailing was produced to required standards. They don't offer time-stamped visibility into serialized mail pieces and their contents.

- Delays and missed deadlines. With third-party fulfillment houses, there is no way of knowing when mail was actually produced or when it was inducted into USPS. This creates uncertainties around timely delivery.

- No consistency. Fulfillment houses often use manual labor to prepare mail pieces, which means the quality may vary. One mailing might be high quality and delivered on time, while the next one may be poorly prepared or delivered late.

  Moreover, mailings may be co-mingled to optimize production queues or postal discounts, which can compromise the quality of a mail run.

- Security breaches. Giving a customer database and regulated consumer information to a third party increases the risk of data theft and security violations. A disreputable outsourcing company may steal a mailing list and sell it. There is also the risk of consumer information, such as Social Security numbers, falling into the wrong hands.

Ultimately, any organization will be held accountable for any regulation violations or security breaches. Put another way, while

it is possible to outsource the work, it isn't possible to outsource the responsibility.

3.0 IS YOUR ORGANIZATION COMPLIANT?

All mailers need to ensure that they are protecting customers' personal information and are in compliance with government regulations.

HERE ARE THREE QUESTIONS THAT WILL HELP DETERMINE IF YOUR ORGANIZATION IS COMPLIANT:

- Does hard-copy mail have comparable safeguards and level of security as electronic communications?
- Is there on-demand visibility into each mail piece?
- Does an audit trail exist for each mail piece for quality assurance (either in-house or as it's being sorted at the post office)?

If the answer is not "yes" to all of these questions, don't panic. Instead, take it as an opportunity to implement best practices for mailing compliance.

4.0 BEST PRACTICES FOR MAILING COMPLIANCE

Whether an organization outsources mailing services or handles everything in-house, there are a number of best practices that can help reduce the associated compliance risks. Here are some tips and technical solutions that will keep an organization in compliance:

4.1 Outsourcing Best Practices

Make sure that an outsourcing service maintains the following industry standard certifications:

- Service Organization Control (SOC) No. 2/3. According to the SAS website, a SAS 2/3 Audit "shows that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes."

...mailings handled by certified providers will meet the highest quality and security standards.

- International Organization for Standardization (ISO). The ISO is the world's largest developer and publisher of international standards. Since ISO is a globally-recognized standard, it is important that any outsourcing service provider maintains this certification.

- Mail Preparation Total Quality Management. According to USPS, this "program is designed to help businesses prepare mailings that meet or exceed Postal Service™ processing quality standards."

Although pricing quotations from companies with these certifications are typically higher than quotes from non-certified fulfillment houses, mailings handled by certified providers will meet the highest quality and security standards.

4.2 In-house Mail Preparation Best Practices

For organizations handling mailings in-house, visibility and quality controls ensure and track the integrity and successful completion of every mail piece – whether they are produced internally or inducted at the post office. For example, 2D input- and exit-scanning technology not only embeds handling instructions into mailings, but also serializes each mail piece and its contents for closed-loop tracking and reporting.

Additionally, technology such as USPS Intelligent Mail barcode (IMB) can give great visibility into mailings. Most companies use IMBs to receive postage discounts. However, USPS also allows them to be used to trace mail through the postal system, so it is possible to know where any mail piece is at any given time.

To comply with SOX, organizations must accurately track the postage spend for each mailing. This not only produces a paper trail for compliance, but also creates an opportunity for savings, as mailing expenditures can be charged back to different internal departments or cost centers.

4.3. Understand the Full Cost of Your Mailing

Whether mail preparation is done in-house or outsourced, understanding the full cost of the finished mail piece is critical. Remember, the total cost is much more than just the postage – it includes everything from envelopes to ink to manual labor and postage. Since fulfillment houses need to mark up the

entire mail process, the cost of outsourcing will always be more expensive than doing it in-house.

5.0 TALK TO PITNEY BOWES

Government and industry regulations can affect any business and create risk. However, using the right best practices, processes, technology and services can minimize these risks while creating more efficient mailing operations.

This resource is intended as a high-level look at mailing regulations and best practices on how to comply. If you'd like to learn more about your organization's risk profile and how to abide by your industry's regulations, don't hesitate to contact a Pitney Bowes representative.

For more information please vist:
http://www.pb.com/equipment/

Pitney Bowes