

Top Security Considerations When Choosing a Lockbox Service Vendor



Lockbox security concerns on the rise

Secure payments continue to be top of mind for many companies as risks of fraud and data breaches are on the rise. According to a recent Strategic Treasurer survey, nearly one-third of corporations noted an elevated uptick in significant threats in 2022.¹

How can your corporation assess potential lockbox vendors to make sure you're getting all the support you need from a product and security standpoint? Focus in on the following considerations to get started. There's also a list of questions to ask potential lockbox providers at the end of this eBook.

Certain parts of the lockbox process, such as exception processing, have experienced an increased focus on security. Due to hybrid work environments, many businesses have had to transition exception processing to home-based employees. This creates information privacy and regulatory compliance concerns for many organizations.



There are several considerations to keep top of mind when assessing a potential lockbox provider:

1. Information Security Policy
2. Third-Party Risk Assessment
3. Compliance
4. Employee Security Training
5. Industry Experience



Information Security Policy

Lockbox providers should safeguard business information, payment data and assets from unauthorized access. The policies and procedures in place to keep this information and data secure is known as an Information Security Policy.

In recent months, these policies have become important as companies expand and many payment processes are being performed by offshore companies. “Some countries are considered riskier to do business with, and that’s why clients are asking if any part of our process is performed overseas,” says Sarah Mille, senior product manager of Deluxe Lockbox

“At Deluxe,
we see our
vendors as
an extension
of ourselves.”

Third-Party Risk Assessment

Companies are not only interested in their immediate lockbox provider, but also the third- and fourth-party vendors they use to complete lockbox processing. Particularly for banks, who need to abide by strict federal regulations, third-party risk management is important. Theodore Sanchious, vice president and director of payments solution consulting at Deluxe, shares one example of a fourth-party vendor: A shredding vendor that a lockbox provider uses picks up the mail at the post office to be properly disposed of. In this scenario, Sanchious details that companies want to know the specifics about this shredding vendor and how the lockbox provider is managing that vendor as part of its secure, ongoing process.

“Our clients want to know that we are managing our vendors (known as fourth-parties) appropriately. Banks especially have a concern as they are governed by the OCC. They also want assurances that we, ourselves, have control of our processes,” explains Sanchious. “At Deluxe, we view the vendors that we use as an extension of ourselves.”





Compliance

Your lockbox provider should follow regulated compliance standards for information and data security. This includes conducting regular self-assessments and external auditor examinations. For example, Payment Card Industry (PCI) certification by the Security Standards Council has a set of requirements a lockbox provider must comply with to secure your company's card data. Some of these requirements include firewall installation, data encryption and anti-virus software. "PCI certification is especially important for our credit card processing customers," adds Mille.

Additional compliance practices include Six Sigma-driven quality assurance. The ability to track mail and transaction content from post office to completion enables a lockbox vendor to provide the highest possible service quality to its clients.

A lockbox provider should also be SOC 1 certified. Regulated by the American Institute of CPAs (AICPA), System and Organization Controls (SOC) audits verify that a service provider is compliant in five areas: security, availability, processing integrity, confidentiality and privacy controls. SSAE SOC 1 Type 2 audits (often conducted annually) "report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls."²

Compliance also extends into the physical existence of the lockbox processing locations. Are cameras and video surveillance being used? A trusted lockbox service provider should use both methods. The use of biometrics and ID cards, finger printing, background checks and employee training can also be important considerations to uphold security.



Employee Security Training

Building off physical site security, employee training is key to reaching a consistent level of information and data security. Both managers and data-owner employees go through training and experience different levels of access based on their unique roles in lockbox processes. According to 2022 Strategic Treasurer survey data, 78% of companies indicated “employee education” as a current control in place to prevent fraud.¹

“Lockbox clients want to know that their provider is doing background checks as well. They want to make sure that the people that we’re hiring are trustworthy and that they are not convicted criminals,” says Mille. “They want to know we’re training them appropriately and that we aren’t allowing cell phones on the floor where they could take pictures of confidential information.”

In addition to training, employee education and policies, such as a cell phone-free policy and code of conduct handling sensitive payment information, should be regularly updated and ongoing. Access Control Policy and Authentication Standards also help keep formal processes in place for managers and data owners to grant approval and/or terminate access at physical lockbox processing locations.



78%

of companies indicated “employee education” as a current control in place to prevent fraud.¹





Industry Experience

By working with a vendor that has existing experience in the lockbox operations space, a company can feel confident that security practices have adapted and remained consistent, but scalable, through the years.

“Lockboxes have been around for the past 50 years. Deluxe is one of the few non-financial institution in the marketplace,” says Sanchious. “More than 65 percent of all lockbox transactions in the U.S. are currently processed using Deluxe software.”

Deluxe has been running lockbox operations for more than 25 years and providing lockbox-related software and professional services to the payments industry since 1974 – more than 45 years of continuous industry expertise. Deluxe currently works with more than 14,000 organizations across our entire Deluxe network.



What steps should a company take to add a lockbox vendor?

A company or financial institution looking to add a lockbox vendor would likely evaluate a vendor through either a Request for Information (RFI) which is typically a request for high-level capabilities to determine if the vendor is a good fit for the company and can meet their objectives or a Request for Proposal (RFP) which is a detailed request for information about the company and its capabilities (inclusive of pricing).

Through the RFI and/or RFP process, the company should determine and evaluate if the vendor has:

A competitive solution:

- » Full spectrum of services
- » Nationwide network of processing locations
- » Robust & flexible reporting options

Flexible processing capabilities:

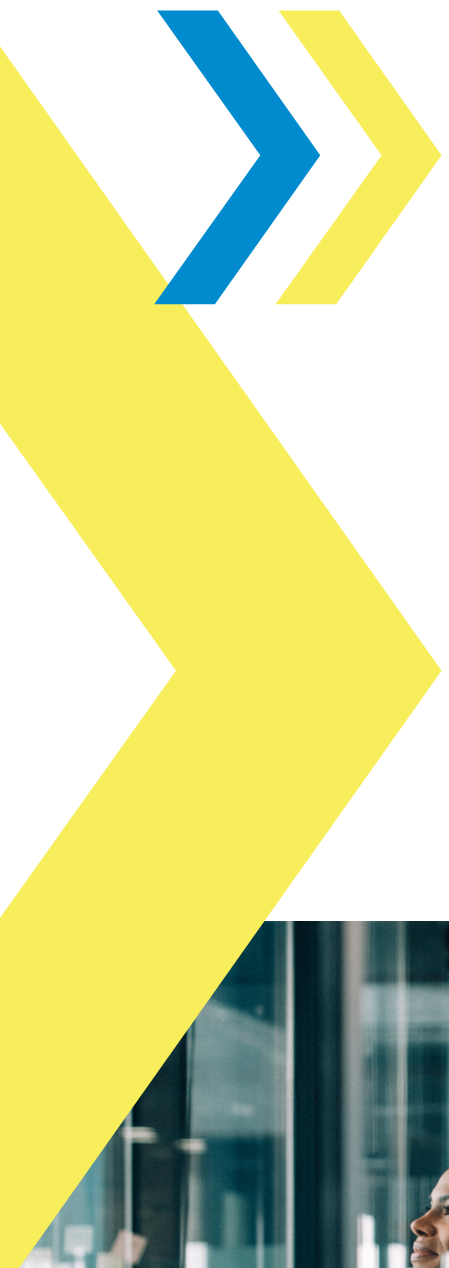
- » Retail, wholesale, wholeetail
- » From plain vanilla to very customized processing
- » Remittances can be scanned
- » Remittance data can be key entered and transmitted

Robust online access:

- » Image archive available 24/7
- » Single sign-on Capabilities
- » Secure access via entitlements
- » Multi-factor authentication

Secure processing:

- » Held to the highest security and compliance standards
- » Comprehensive BCP including testing
- » Adherence to Service Level Agreements (SLAs)



Take the steps today for secure lockbox processing tomorrow

When assessing security, you want a lockbox provider that is regulated and uses industry best practices for development, security, and all aspects of client service. From third-party risk assessment and information security policies to consistent employee training and industry-leading experience, your lockbox provider should help provide peace of mind and secure processing every step of the way.

“As a strategic partner for lockbox services, Deluxe’s goal will always be to offer a large-scale, proven array of receivables services that directly match a company’s required and desired capabilities for lockbox processing,” says Sanchious.





About Deluxe

Deluxe, a Trusted Payments and Data Company, champions business so communities thrive. Our solutions help businesses pay, get paid, and grow. For more than 100 years, Deluxe customers have relied on our solutions and platforms at all stages of their lifecycle, from start-up to maturity. Our powerful scale supports millions of small businesses, thousands of vital financial institutions and hundreds of the world's largest consumer brands, while processing approximately \$3 trillion in annual payment volume. Our reach, scale and distribution channels position Deluxe to be our customers' most trusted business partner. To learn how we can help your business, visit us at www.deluxe.com.

Checklist: Top security questions to ask when choosing a lockbox provider

Choosing the right lockbox provider is an essential part of helping to ensure your payments are processed with efficiency, security and accuracy. To get started, here are common questions to ask your vendor when considering their lockbox offerings:

- ☐ Are you subject to FFIEC audit?
- ☐ Do you have a robust third-party risk management process?
- ☐ Do you perform SSAE 18 SOC II Type 2 Audit annually?
- ☐ Are you PCI Certified/Compliant?
- ☐ Are you HIPAA compliant?
- ☐ Do your employees receive HIPAA Training? If so, how often?
- ☐ Do you provide third-party attestation?
- ☐ Do you perform Vulnerability – Penetration Security Assessments on your web applications?
- ☐ Do you utilize offshore data entry or other resources ?
- ☐ Can you share your Software Development Life Cycle Practices?
- ☐ Do you have employee/associate Confidentiality Agreements?
- ☐ What is your Business Continuity Plan (BCP), and can we see a copy?
- ☐ Please provide your Disaster Recovery Testing Results. Do you perform Annual Testing?
- ☐ Provide an overview of your Hiring – Transfer – Exit Procedures for employees.
- ☐ Do you have an employee security training program?
- ☐ Do you perform employee background checks? If so, how often?
- ☐ Are your processing locations equipped with cameras and/or video technology? What type of cameras/video technology are used?