IN.gov

Empowering Agencies: A Comprehensive Guide to IN.gov's Payment Processing Program

June 30th, 2023

IOT
Indiana Office of Technology
Powering a State that Works

www.in.gov/iot

Payment Processing with IOT

The State of Indiana holds Quantity Purchase Agreements (QPAs) with two Indiana Government payment processing services vendors: Tyler Indiana and Value Payment Systems (VPS). The Indiana Office of Technology (IOT) manages both contracts. Safe, secure payment processing through the State's contracted vendors is of great value to State and Local Government agencies. Payments are processed quickly and accurately, allowing agencies to receive funds promptly. This builds trust between the government and its agencies and provides transparency in the payment process, allowing agencies to track the status of their payments while ensuring they are paid fairly and accurately. Lastly, protecting sensitive financial information from fraud and other forms of cybercrime is essential.

As of June 2023, forty-eight State agencies and eighteen Local Government agencies have payment processing services via one of the State's payment processing vendors. IOT's support is primarily towards new services, outreach, and escalation. IOT conducts monthly business reviews with each vendor to discuss all ongoing projects, tickets, initiatives, and any issues or escalations. Day to day, the IOT team is the facilitator for agencies seeking a new service and serves as an escalation channel if an agency needs assistance with one of the vendors.

This paper will provide historical information regarding the establishment of the state's payment processing program, define the benefits of participation, touch on compliance with industry standards, and provide information regarding assurance to agencies that they have chosen the right payment processor to fit their needs.

Beginnings and Development

In 2005 as part of IOT's statutory formation, it was conferred the responsibility of managing payment processing for the State. First, Legislature established that state agencies could accept electronic payments online, specifically via the "computer gateway administered by the office of technology" (State and Local Administration, Electronic payment, IC 5-27-3-1 (2022)).

In addition, IC 5-27-3-2 specified that state government agencies must use the payment processor provided by IOT for all forms of electronic payment, which are defined to include credit and debit card payments, not necessarily just those made online (State and Local Administration, Electronic payment definition, IC 5-27-3-2 (2022)).

Prior to 2017, payment processing at the State of Indiana consisted of a Quantity Purchase Agreement (QPA) as well as a handful of independent contracts signed directly with the agencies (QPA # 12949, Master Services Agreement (2012)). With the 2017 Portal Services Contract including payment processing, there were now two standard offerings across the state: VPS via IDOA and Tyler Indiana via IOT's IN.gov program. VPS with IDOA was the primary QPA for payment processing services, whereas agencies received Tyler Indiana services as an

additional service via IOT IN.gov. With coordination between IDOA and IOT, the VPS contract transitioned from IDOA to IOT management in 2021.

IOT issued an RFP in 2021 that concluded in October 2021, with both the incumbents, VPS and Tyler Indiana, awarded the new contracts. The new payment processing contracts included more services and lower fee rates across the board. The new contracts went into effect in October 2022 after a one-year transition period (QPA # 59726, Master Services Agreement (2022), QPA # 59725, Master Services Agreement (2022)).

Basic Benefits

In addition to being mandated by Indiana statute to be the stewards of payment processing for the State, IOT manages the payment processing contracts to provide the following benefits:

- **Compliance:** The State of Indiana has its own laws, regulations, and procurement policies governing financial transactions. IOT ensures that payment processing contracts comply with state-specific requirements, including transparency, accountability, and adherence to procurement guidelines. To strengthen agency insight into the payment processing statute, IOT issued a statewide policy in the State's governance, risk and compliance portal.
- **Cost Efficiency:** Enterprise payment processing enables the IOT to negotiate and procure competitive rates and terms with vendors, compared with one-off contracts. After the recent RFP, vendor rates were significantly reduced to benefit government customers.
- **Tailoring to Agency Needs:** Each agency has unique requirements and priorities based on its government operations, industry landscape, and financial transactions. IOT serves as a facilitator introducing Agencies to the payment processing vendors and ensuring each Agency receives tailored services.
- **Vendor Relationships:** IOT has a dedicated team to manage the payment processing vendor relationships, allowing the team to build solid and trusted relationships with both vendors. The IOT team communicates daily with both vendors and meets with each regularly to review all ongoing tickets and projects and proactively manage any issues. The relationships IOT has built with both vendors has contributed to efficient and effective service delivery from vendors to State and local agencies.

Compliance - Payment Card Industry (PCI)

It is important to maintain Payment Card Industry (PCI) compliance, which credit card companies mandate to help ensure the security of credit card transactions in the payments industry.

PCI compliance refers to the technical and operational standards the selected vendors follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions. PCI standards for compliance are developed and managed by the PCI Security Standards Council.

Both of the state's payment processing vendors have years of experience in government payment technology and have proven they meet the twelve requirements of the PCI Data Security Standard:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

(PCI Security Standards Council. (2018, July). PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved June 14, 2023. https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf)

Fine Tuning Payment Processing Selection– Secondary Competitive Process

With the start of the new Payment Processing QPA with two vendors, IOT introduced the Secondary Competitive Process (SCP). This is used in two situations: when an agency with no prior payment processing needs service and when an agency with an existing payment processing service and relationship wants to explore switching vendors. The two vendors have

already completed a competitive bidding process for the QPA, hence the name "Secondary" Competitive Process.

The SCP is initiated by an agency requesting more information from IOT regarding payment processing options. The IOT Payment Processing team sends the agency a pre-designed Statement of Work (SOW) template, in which the agency details its payment processing needs and requirements. IOT passes the SOW to both payment processors, who have a defined amount of time to ask questions and provide an implementation plan, including a detailed timeline, any subcontractors, and a high-level project plan. The agency can choose a processor based upon the implementation plan or request oral presentations. After the oral proposal, the agency notifies IOT of its selection.

Offering both vendors the same SOW and requirements and viewing the implementation plans side-by-side helps the agency more clearly evaluate its options.

Conclusion

Safe payment processing via the State of Indiana contracts is essential for ensuring that government procurement processes run smoothly and efficiently. The government and its vendors can benefit from increased trust, compliance, and efficiency by providing a secure and transparent payment process.

As agencies seek to streamline operations, more are turning to IOT's payment processing vendors for retail needs at events, such as the Indianapolis Boat, Sport, and Travel Show and Indiana State Fair Indiana Grown retail store. The payment processing program is an example of how IOT continues to focus on offering innovative services for its customer agencies and their constituents.