IntelliPay®

City in the Cloud
County in the Cloud

Local Government Payments Decision Making Guide

About this Guide

If you're reading this, you're probably somewhere on the spectrum between "we just started taking card payments" and "we know something better is out there." Either way, you're in the right place.

This guide walks you through every major decision your agency will face when evaluating electronic payment processing — from who pays the fees, to which channels make the most sense, to what questions to ask a vendor.

It's designed to cut through the industry jargon and help you make a confident, informed choice for your community.

One important note upfront: there is no single perfect payment solution. If there were, every government agency in the country would be using it and every other vendor would be out of business. What matters is finding the right fit for your agency, your constituents, and your budget.

Alot has changed in the last five years

The government payments landscape has shifted significantly in recent years. Here's why updating your knowledge matters right now:

Federal mandate for digital payments: In March 2025, [Executive Order 14247](https://www.whitehouse.gov/presidential-actions/2025/03/modernizing-payments-to-and-from-americas-bank-account/) required all federal agencies to stop issuing paper checks by September 30, 2025. State and local governments are under increasing pressure — and financial incentive — to follow suit, since roughly 36% of state revenue comes from federal dollars.

PCI DSS 4.0 is now fully enforced: As of March 31, 2025, the new Payment Card Industry Data Security Standard (PCI DSS version 4.0) became mandatory. This is the biggest update to payment security requirements in over a decade, with 64 new requirements. Your processor needs to be on top of this — and so do you.

Constituents expect digital options: Constituents expect digital options: 93% say governments should offer electronic payments; 88% would pay electronically if given the chance. U.S. card volume reached $11.46 trillion in 2025 — up 6.4%, outpacing 2024 growth — proving constituent demand keeps accelerating. (Nilson Report)

Interchange fees are shifting: Interchange fees are shifting: Visa and Mastercard's antitrust case remains unresolved; a $38B settlement capping rates at 1.25% is still unapproved and actively opposed by major merchant groups. Meanwhile, U.S. card volume grew 6.4% to $11.46 trillion in 2025 — faster than 2024 — proving interchange isn't going away. Even PayPal, Stripe, and Cash App run on card rails. Your fee model choice matters more than ever.

Step One: Decide who pays the processing fees

This is the most important strategic decision your agency will make. Everything else flows from it.

Here's the honest truth: electronic payment processing is never free. Someone always pays for it. The question is whether that cost is absorbed by your agency's budget — and therefore by all taxpayers — or passed along only to the constituents who choose to pay electronically.

Think of it like a restaurant: the menu prices already include the cost of card processing. People who pay cash are essentially subsidizing the card users. Government agencies face the same dynamic.

You have two main paths:

Path 1: Traditional processing (Agency pays the fees)

With traditional processing, your agency covers the cost of accepting electronic payments. Constituents pay nothing extra.

How the fees break down:
There are typically two types of costs:

1. Monthly fixed fees: These are baseline charges just for having the ability to accept payments (like a gateway fee or account maintenance fee).

2. Interchange costs :These are the fees set by Visa, Mastercard, Discover, and American Express for each transaction. Think of interchange as the wholesale cost of credit card processing.

The way processors charge you for interchange varies:

Tiered pricing: Your processor groups cards into buckets (qualified, mid-qualified, non-qualified) and charges a fixed percentage for each. The problem? You never really know what the underlying cost is, and processors have wide latitude to define the tiers in their favor.

Interchange-plus pricing: Your processor passes the actual cost from the card networks directly to you, then adds a small, transparent markup. This is more transparent and typically more predictable. It's the model to ask for.

What should you expect to pay?

Typically between 2% and 3% of your total processing volume - closer to 2% for in-person (card-present) transactions and closer to 3% for online or phone (card-not-present) payments, and for premium rewards cards.

The trade-off:

Traditional processing is simple and familiar — constituents aren't surprised by any fee at checkout. But it means your agency is voluntarily redirecting 2–3% of taxpayer dollars away from services like road maintenance, parks, and public safety. Some agencies with budget surpluses are comfortable with this trade-off. Many are not.

Path 2: Service fee processing (Constituent pays the fee)

This model makes electronic payment processing effectively cost-free for your agency. The fee is charged to the constituent who chooses to pay with credit card and that fee is used to cover the cost of processing.

This is also called "revenue-neutral", because your agency receives 100% of what's owed, with no processing costs coming out of your budget.

Paying by the card brand rules

Visa, Mastercard, American Express, and Discover each have their own rules governing how merchants can pass payment processing costs to cardholders. Understanding these rules — and the terminology each network uses — is essential to staying compliant and avoiding fines or program termination.

What the Card Networks Call It

The term you use matters because it determines which set of network rules apply. Each card network has its own name for its government and utility fee program:

Card Network	Term Used	Transaction Share (2025)
Visa	Service fee	~50%
Mastercard	Convenience fee	~25%
American Express	Convenience fee	~15%
Discover	Either term is acceptable	~8%

Visa leads U.S. card transactions — 30% of credit, 31% of debit (Nilson Report, Feb. 2026) — and because it's the dominant network, its term "service fee" is most common in government payment contexts. However, Mastercard calls its program a "convenience fee," meaning agencies must comply with both sets of rules simultaneously. These programs have meaningfully different requirements.

Convenience Fee Rules (Mastercard, Amex, Discover — and Visa for Non-Eligible Merchants)

A convenience fee compensates the merchant for offering an alternative payment channel — such as an online portal when the standard channel is in-person or by mail. Both Visa and Mastercard impose the following conditions for a valid convenience fee:

- Must be a flat, fixed dollar amount — never a percentage of the transaction
- Can only be charged when a true alternative payment channel exists (e.g., paying online when the normal method is at a counter or by mail)

Convenience fee rules cont.

- Cannot be charged in a face-to-face (card-present) environment
- Cannot be charged for recurring payments (subscriptions, utility auto-pay, etc.)
- Must apply equally to all payment methods within that channel — not just cards
- Must be disclosed before transaction completion, with the cardholder given the option to cancel

A merchant that accepts only card payments (100% card-not-present) cannot charge a convenience fee — there is no "alternative" channel to justify it

The flat-fee requirement is a practical limitation for utilities: a fixed $2.00 fee covers costs on a $50 bill but falls well short on a $500 commercial account. This is a key reason the service fee model exists.

Service fee rules (Visa — and now utilities)

Service fees are more flexible than convenience fees but are available only to a narrower set of merchants. Key rules under Visa's service fee program:

- Eligible merchant categories: government, education, and — as of October 18, 2025 — utilities (MCC 4900)
- Can be fixed or variable (percentage-based), unlike convenience fees — this enables full cost recovery on high-dollar bills
- Visa no longer requires merchants to register before implementing a service fee (registration requirement removed October 2025)
- Fee amount must be disclosed to the cardholder before the transaction is completed

Typically implemented using a Two-MID structure (two separate Merchant Identification Numbers), though implementation details vary by processor and acquirer

How the Two-MID structure works:

The merchant operates two accounts — the first MID receives the constituent's payment and deposits it directly into the agency's bank account; the second MID collects the service fee and deposits it into the processor's account to cover transaction costs for both.

For example: a constituent pays a $100 water bill with a 2.5% service fee. The constituent pays $102.50 total. The agency receives $100.00. The processor receives $2.50 and applies it against processing costs.

Important Limitations and Conflicts

Even if your agency qualifies for the service fee or convenience fee program, two additional restrictions may apply:

1. Visa's Utility Interchange Rate Program

If your agency participates in Visa's lower utility interchange rate program, that program requires waiving all cardholder fees entirely. This makes the utility interchange rate and any cardholder fee program (service fee or convenience fee) mutually exclusive you can have lower interchange or a fee pass-through, but not both.

2. State Public Utility Commission Rules

Many state PUCs have their own restrictions on what fees utilities may charge ratepayers, independent of card network rules. State rules may prohibit percentage-based fees, cap fee amounts, or restrict fee programs to specific payment channels. These restrictions apply in addition to card network rules, and the more restrictive rule governs.

Is a service fee right for your agency?

Ask yourself: Would your constituents rather pay a modest fee to pay electronically at their convenience — online, by phone, at a kiosk — or do you want to absorb that cost across all taxpayers, including those who pay by cash or check? For most agencies, the service fee model is both fiscally responsible and widely accepted by constituents when it's clearly communicated upfront.

Step Two: Choose how you'll accept payments

Once you've decided on your fee model, the next step is figuring out which payment channels you need. There's no single right answer — it depends on your agency's size, the types of payments you collect, your staff capacity, and where your constituents prefer to pay.

Modern government payment platforms support a full range of channels. Here's a plain-language breakdown of each:

In-Person Payments (Card Present)

"Card present" means the constituent is physically at your office or a kiosk, and their card is physically involved in the transaction — whether that's inserting a chip card, tapping a contactless card or phone, or swiping.

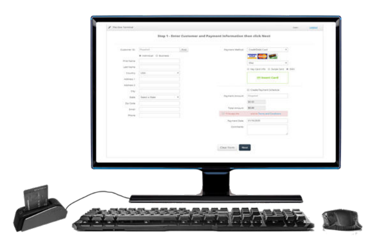
Why it matters: Card-present transactions carry lower interchange rates than online transactions, because the risk of fraud is lower when the card and cardholder are in the same place.

.

Your equipment options:

Standalone Payment Terminal

A dedicated device with a screen and keypad similar to what you see at a grocery store checkout. Best when there's no computer nearby for staff to use, or when you need to share a single device across multiple employees. Modern terminals also accept contactless payments (tap-to-pay) via cards and digital wallets.



Computer-Connected Card Reader

A card reader that plugs into a USB port on an internet-connected computer and works through a virtual terminal (a web-based interface your staff uses to process payments). This is the most common setup for government office counters because it integrates well with your existing computers.

Mobile Device

A card reader that connects to a smartphone or tablet via Bluetooth or USB. Ideal for field collections, pop-up payment events, or any situation where a fixed terminal isn't practical. The staff member downloads a payment app, and the reader becomes a portable point-of-sale.

Payment Kiosk

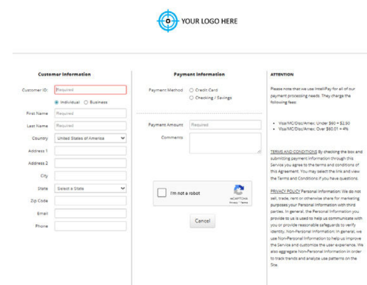
A self-service station — often placed in a lobby or public-facing area — that lets constituents pay on their own without staff involvement. Kiosks are particularly effective for after-hours payments and high-volume locations like courthouses, utility offices, or government centers.

Online and Remote Payments (Card Not Present)

“Card not present” covers any transaction where neither the constituent nor the physical card is in your office - online

Online Payment Portal

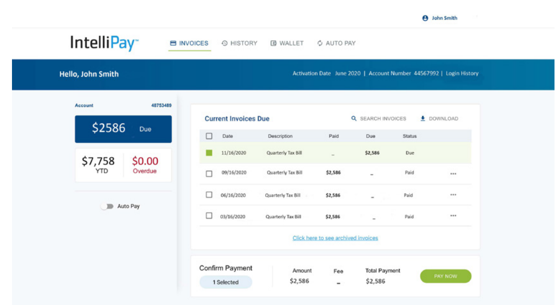
The most common starting point. Your agency’s website includes a link to a secure, branded payment page where constituents can make a one-time payment. The page looks and feels like your agency’s site, but the transaction happens on your processor’s secure server — which is actually a security advantage, since it keeps cardholder data off your systems entirely.



Customer Self-Service Portal

A more robust option that allows constituents to log in with their own account, view their current balance or bill history, make a payment, and set up recurring payments. This is particularly use-ful for utilities, courts, and any department that collects regular recurring payments from the same constituents.

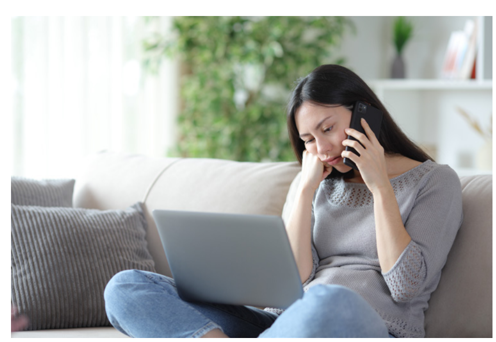
IntelliPay’s portal lets constituents pay for multiple items in a single transaction, for example, a business paying for multiple permits, or a citizen paying both a parking fine and a registration renewal.



IVR Phone Payments (Automated Phone System)

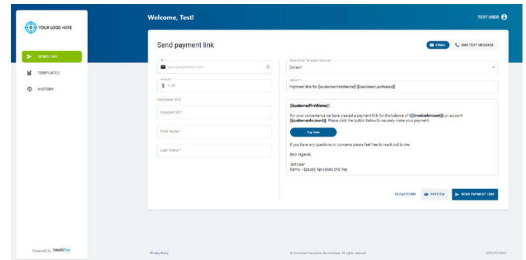
An Interactive Voice Response (IVR) system lets constituents call a phone number and complete a payment through an automated menu without waiting for a staff member. The constituent enters their account information and payment details using their phone keypad.

This is a high-value option for reducing call center load while still serving constituents who prefer phone transactions or don’t have reliable internet access.



Text-to-Pay

Your agency sends a text message to the constituent's mobile phone with a secure payment link. One tap opens the payment page. Particularly effective for utility bills, court payments, and other recurring notifications. Text-to-pay has seen rapid adoption among younger constituents and those who primarily use smartphones.

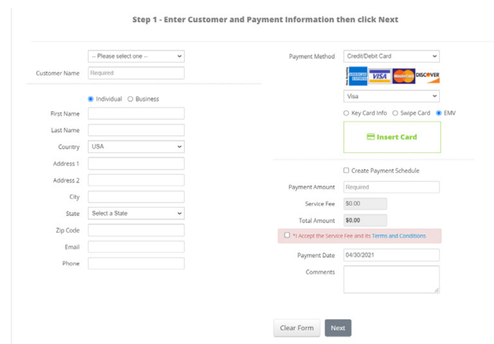


Email-to-Pay

Similar to text-to-pay, but delivered via email. Your staff — or an automated billing system — sends an email with a payment link. The constituent clicks and pays without needing to log in to a separate portal or call your office. This reduces inbound phone calls significantly.

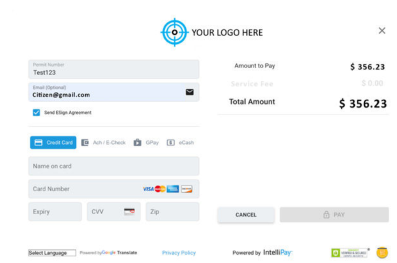
Virtual Terminal (Staff-Assisted Phone Payments)

A web browser-based interface your staff uses to manually enter payment details when a constituent calls in to pay by phone. The cardholder reads their card number over the phone; the staff member enters it. This is different from IVR — it requires a live staff member but gives you full flexibility for any transaction type.



Lightbox / Embedded Payment Modal

A payment window that appears directly on top of your existing software or website, giving the appearance of a fully integrated payment experience without requiring a full technical integration. The constituent never feels like they've left your site. This is a practical bridge solution when your fund management software doesn't yet offer a direct payment integration.



Step Three: Decide how much to automate (Integration Level)

Once you've settled on your fee model and your payment channels, the final major decision is how tightly you want your payment system to connect with your existing government software.

There are two integration levels:

Semi-Integration

A semi-integration is a practical middle ground when a full technical connection isn't possible or cost-effective. For example, your fund management software might allow you to export a billing file that gets uploaded into a payment portal and constituents can then look up their account and pay online. There's a manual step involved (downloading and uploading files), but from the constituent's perspective, the experience can look and feel like a full integration.

A lightbox modal (described above) is another semi-integration approach; the constituent appears to stay on your site, but is actually on a secure payment page.

When semi-integration makes sense:

Your current software vendor charges expensive integration fees, your agency doesn't have internal IT capacity for a full integration project, or you need to get something operational quickly.

Full integration

A full integration means your payment system and your fund management or ERP software talk to each other in real time. When a constituent makes a payment, it's immediately reflected in your system — no manual file uploads, no reconciliation gaps, no double-entry.

Full integration is the gold standard for efficiency. It reduces staff workload, eliminates errors, and gives your finance team a real-time view of collections.

What to watch out for:

Some software vendors charge significant fees or refuse to open their system up to third-party payment processors. Push back on this and look for payment processors with a wide library of existing integrations. IntelliPay, for example, has integrations with over 200 government software platforms, which means the heavy lifting may already be done.

One thing to know about EMV and chip cards:

If you're using a service fee model with in-person card-present transactions, ask your processor about single-dip EMV processing. Traditional two-MID service fee setups require a chip card to be inserted twice (once for each merchant account). Patented technology exists that allows this to happen in a single chip card insertion a better experience for your staff and constituents.

Step Four: Understand cloud-based payment processing

If you've modernized other government systems in recent years — your ERP, your document management, your email — you've probably moved at least partially to the cloud. Your payment processing should be no different.

Here's what cloud-based payment processing actually means for your agency:

Security you don't have to manage yourself

Cloud-based payment processors maintain their security infrastructure to the highest PCI DSS standards (currently version 4.0, which became mandatory in March 2025). By processing transactions on the processor's secure network rather than your own systems, you dramatically reduce your agency's compliance burden. You're not storing card numbers. You're not responsible for the server infrastructure that handles sensitive cardholder data

PCI DSS Level 1 compliance

The highest tier; requires annual on-site audits by a certified assessor and quarterly network scans. The best processors maintain this certification so their government clients don't have to do it independently.

Always available

Constituents don't keep business hours. They pay utility bills at 10pm, parking fines on weekends, and recreation fees during their lunch break. A cloud-based payment platform with 99.99% uptime means your payment portal is available when your constituents need it — not just when your office is open.

No software to install or update

Cloud-based platforms update automatically. Your staff always has access to the latest features and security patches without IT projects or downtime windows. New payment methods — like emerging digital wallets or real-time payment rails — can be added without replacing your core system.

Access from anywhere

Any authorized staff member can run reports, look up transactions, or process a payment from any internet-connected device. This is particularly useful for multi-department agencies, remote staff, or administrators who need visibility across multiple locations.

Built-in fraud detection

Modern cloud payment platforms use AI-powered fraud detection that analyzes transaction patterns in real time and flags suspicious activity before it becomes a problem. IntelliPay's platform, for example, has reduced fraudulent transactions by 87% for partner agencies through these tools.

Implementation: What to Expect

A common concern we hear from government agencies is that switching payment processors or implementing electronic payments for the first time will be a major disruptive project. Here's a realistic picture:

Timeline: Most agencies are fully operational with a new payment system within 45 to 60 days from contract signing. That assumes a standard implementation; agencies requiring custom integrations or significant customization may take longer.

What you'll need to provide: Your agency's bank account information for fund deposits, your existing software vendor contact (for integration discussions), any branding assets (logo, color scheme) for customized payment pages, and department-level contacts for training.

Staff training: Modern cloud-based platforms are designed to be intuitive. Most agencies find that counter staff can become comfortable with the system in a few hours, not days.

Going live: A phased rollout — starting with online payments before adding in-person channels, for example — can reduce risk and give staff time to get comfortable before full deployment.

Questions to Ask Every Vendor

Not all government payment processors are the same. Use these questions to evaluate any vendor you're considering:

Pricing and Fees

- What is your pricing model — tiered or interchange-plus?
- Are there monthly minimums, gateway fees, or per-transaction fees in addition to interchange?
- What is the total cost as a percentage of my expected processing volume?
- If we use a service fee model, what fee percentage or flat fee will constituents pay? Is it variable or fixed?
- Are there fees to set up or terminate the contract?

Compliance and Security

- Are you PCI DSS Level 1 certified? Can you provide your current Attestation of Compliance (AOC)?
- Are your terminals and card readers P2PE-validated (Point-to-Point Encrypted)? (P2PE encrypts card data the moment the card is inserted or tapped, before it ever reaches your network.)
- Do you support EMV chip card processing?
- What fraud prevention tools do you offer?

Integration and Technology

- How many government fund management and ERP systems do you integrate with?
- What does an integration with our current software require, and is there a cost?
- Do you offer a semi-integration option (like a lightbox modal or file-based batch upload) if a full integration isn't feasible?
- Do you support digital wallets (Apple Pay, Google Pay)?
- Do you support ACH and eCheck payments?
- Is your platform accessible on mobile devices for constituents?

Service and Support

- What are your support hours, and how do constituents reach you if they have a payment question?
- Do you offer a dedicated government account manager?
- Is your support team U.S. based?
- What is your average response time to emails, calls, text?
- Can you provide references from other local government clients similar in size to our agency?

Contract Terms

- What is the contract length?
- Is there an auto-renewal clause, and how much notice is required to cancel?
- Are there volume commitments or penalties for processing below a threshold?

Decision-Making Checklist

Use this checklist as you move through the evaluation process:

Fee Model

[ ] We have reviewed our current processing costs (if applicable)
[ ] We have decided whether our agency or our constituents will pay processing fees
[ ] We understand the difference between a service fee (Two-MID) and traditional processing
[ ] We have confirmed whether any state laws or regulations affect our fee model options
[ ] We have considered constituent communication — how will we explain the fee (if any)?

Payment Channels

[ ] We have identified all the departments and payment types we need to support
[ ] We have determined which in-person payment methods we need (terminal, kiosk, mobile)
[ ] We have determined which remote/online payment methods we need (portal, IVR, text, email)
[ ] We have considered how constituents without bank accounts will pay
[ ] We have confirmed whether we need ACH/eCheck in addition to card payments
[ ] We have confirmed whether we need digital wallet support (Apple Pay, Google Pay)

Integration

[ ] We have documented our current fund management or ERP software
[ ] We have contacted our software vendor to ask about payment processor integrations and any associated costs
[ ] We have determined whether a semi-integration or full integration is appropriate for our agency

Security and Compliance

[ ] We understand our PCI DSS compliance obligations
[ ]We have asked prospective vendors for their PCI DSS Level 1 certification documentation
[ ] We have asked about P2PE validation for any physical terminals
[ ] We have asked about AI-powered fraud detection

Vendor Evaluation

[ ] We have gathered proposals from at least two or three vendors
[ ] We have asked all vendors for government-specific client references
[ ] We have reviewed contract terms, including auto-renewal clauses and cancellation terms
[ ] We have confirmed implementation timeline and what our agency needs to provide

Going Live

[ ] We have a plan for staff training
[ ] We have a plan for communicating new payment options to constituents
[ ] We have a phased rollout plan if needed
[ ] We have established who the internal point of contact will be post-implementation

Glossary of Key Terms

ACH (Automated Clearing House)
An electronic network used to move money between bank accounts in the U.S. ACH transfers include direct deposit and eCheck payments. They're typically lower cost than card payments but take one to three business days to settle (though same-day ACH is increasingly available).

Card Not Present (CNP)
Any transaction where the physical card isn't at the point of sale — online payments, phone payments, text-to-pay, and email-to-pay are all card-not-present transactions. CNP transactions generally carry higher interchange rates because fraud risk is higher.

Card Present
A transaction where the cardholder and their physical card are both at the point of sale. Chip card (EMV) transactions, tap-to-pay, and traditional swipe are all card-present. These transactions carry lower interchange rates.

Convenience Fee
A fee charged to a constituent for the convenience of paying through an alternative channel (like online or by phone) that's different from the agency's standard payment method. Under card network rules, a convenience fee must be a flat amount (not a percentage) and must be disclosed clearly before the transaction is completed. Mastercard and American Express use this term for government payment programs; Discover accepts either term.

eCheck (Electronic Check)
A digital version of a paper check. The constituent provides their bank routing number and account number, and the payment is processed as an ACH transaction. eChecks are typically lower cost than card payments.

EMV (Europay, Mastercard, Visa)
The global standard for chip card transactions. EMV chip cards generate a unique transaction code for each purchase, making them far more secure against counterfeit fraud than magnetic stripe cards. EMV is now standard for all in-person card transactions.

Interchange
The fee paid to the cardholder's bank every time a credit or debit card is used. Interchange rates are set by the card networks (Visa, Mastercard, etc.) and vary based on card type, transaction type, and merchant category. This is the largest component of processing costs.

Interchange-Plus Pricing
A transparent pricing model where the processor passes through the exact interchange cost from the card network and then adds a fixed, disclosed markup. Preferred over tiered pricing for its transparency.

IVR (Interactive Voice Response)
An automated phone system that allows constituents to complete transactions by navigating a menu using their phone keypad or voice commands — without speaking to a live staff member.

Lightbox Modal
A payment window that appears overlaid on top of your existing website or software, allowing constituents to complete a payment without appearing to leave your site. A semi-integration approach.

MID (Merchant Identification Number)
A unique number assigned to each merchant account. In a Two-MID service fee setup, one MID receives the constituent's payment and one receives the service fee.

Omnichannel
The ability to accept payments through multiple channels (in-person, online, phone, mobile, kiosk) in a coordinated way, giving constituents flexibility and agencies a unified view of all transactions.

P2PE (Point-to-Point Encryption)
A security standard that encrypts cardholder data at the moment the card is inserted, swiped, or tapped — before it enters any network. P2PE-validated terminals significantly reduce the scope of your agency's PCI compliance requirements.

PCI DSS (Payment Card Industry Data Security Standard)
A set of security requirements established by the card networks to protect cardholder data. PCI DSS version 4.0 became mandatory as of March 31, 2025, and includes 64 new requirements covering multi-factor authentication, continuous risk monitoring, and payment page script security. All merchants and processors that handle cardholder data must comply.

PCI DSS Level 1
The highest tier of PCI compliance, required for processors handling large transaction volumes. Level 1 certification involves annual on-site audits by a Qualified Security Assessor (QSA) and quarterly network vulnerability scans.

Revenue-Neutral Processing
A payment model (typically Two-MID service fee or convenience fee processing) where the government agency pays nothing for electronic payment processing because the fee is covered by the constituent who chooses to pay electronically. The agency receives 100% of the amount owed.

Service Fee
Visa's term for the fee government agencies are permitted to charge constituents for electronic payment processing. Unlike a convenience fee, a service fee can be a percentage of the transaction amount (not just a flat fee). Government and education entities are the primary categories permitted to use this model.

SFTP (Secure File Transfer Protocol)
A secure method of transferring data files between systems. In a semi-integration, a billing file might be exported from your fund management software and uploaded via SFTP to the payment portal.

Tiered Pricing
A pricing model where interchange costs are grouped into tiers (qualified, mid-qualified, non-qualified), and the processor charges a fixed rate for each tier. Less transparent than interchange-plus pricing; the processor has discretion over how cards are categorized.

Two-MID Processing
A payment setup using two separate merchant accounts — one to receive constituent payments, one to receive service or convenience fees. This is the mechanism behind revenue-neutral government payment processing.

Virtual Terminal
A web browser-based application that allows staff to manually enter payment information (typically taken over the phone) to process a card-not-present transaction without a physical card reader.

Summary: Your Path Forward

The good news is that modern government payment processing is more flexible, more secure, and more constituent-friendly than it's ever been. The options available today — service fee programs, digital wallets, IVR, text-to-pay, self-service portals, and AI-powered fraud detection — would have seemed advanced just a few years ago. Now they're standard.

Here's the short version of what this guide recommends:

1. **Start with the fee question.** Revenue-neutral service fee processing is the most fiscally responsible model for most government agencies. It puts 100% of taxpayer dollars back to work while still giving constituents a convenient way to pay electronically.

2. **Build for omnichannel.** Your constituents pay the way they want to pay — online, in person, by phone, by text. A platform that supports all of these channels from a single administration dashboard makes life easier for your staff and better for your community.

3. **Don't underestimate integration.** The difference between a semi-integration and a full integration can be measured in staff hours per week. Ask hard questions about integration options and costs before you sign.

4. **Prioritize security and compliance.** PCI DSS 4.0 is not optional. Choose a processor that maintains Level 1 certification and handles the heavy security lifting on your behalf.

Ready to Talk?

IntelliPay has been serving government agencies for over 20 years — originally as GovTeller, now as IntelliPay. Our platform integrates with more than 200 government software platforms and is built specifically for the compliance, transparency, and constituent experience requirements of local government.

To schedule a free consultation and platform demo, contact us:

Phone: 855-872-6632 x132
Email: sales@intellipay.com
Web: intellipay.com