

ARTICLE

Beyond the card: Why identity assurance is a required layer for payment security and government trust



By Dan Garrett

Director of Market Planning, Payment Solutions, LexisNexis Risk Solutions

There was a time when accepting a card payment meant checking the person, not just the plastic. A cashier would ask to see a driver's license, compare the name, maybe glance at the signature — a simple, human act of confirming that the cardholder was who they claimed to be.

Somewhere along the way, technology stripped that step out. In the name of speed and convenience, we shifted our entire focus to validating the card itself: Does it match the billing address? Is the CVV (card verification value) correct? Does the device look familiar? Does the transaction pattern appear normal or suspicious? These controls help determine whether a payment looks legitimate, and they remain essential.

Yet nowhere does the unanswered question matter more than in government: Is the person behind this transaction truly who they claim to be? After more than three decades in payments and risk, I've become convinced that this gap is doing the most damage — and that's why I believe identity assurance is no longer a back-office control. It's becoming the foundation of trusted payments — not only for commercial businesses but especially for government agencies.

Fraud has evolved beyond stolen card numbers and isolated payment events. Bad actors now exploit compromised accounts, stolen credentials, synthetic identities, trusted devices, and automated tools that can make fraudulent activity appear legitimate at the payment layer. In this environment, a transaction can pass traditional payment checks and still represent material risk.

That is why identity is emerging as the next strategic layer of payment security and why government agencies need to know who is behind every transaction.

Government agencies do far more than accept payments or disburse funds. They control access to public services, official records, permits, licenses, benefits, credentials, and regulated transactions — all while serving as trusted stewards of public funds.

Why government payments require a broader definition of trust

In these settings, the consequences of trusting the wrong person extend well beyond a declined payment, an approved charge, or a chargeback. They can affect program integrity, public confidence, compliance obligations, and an agency's ability to serve the right individual or business with confidence.

Nefarious transactions can provide access to:



Permits, licenses, and professional credentials: An unauthorized person could attempt to pay for, renew, or change a license using information that appears valid at the payment level but does not confirm the applicant's true identity.



Court, citation, and fine payments: A payment may be legitimate, but the person making it may not be the party responsible for the obligation, creating reconciliation, dispute, or record-integrity issues.



Tax, fee, and benefit-related transactions: Agencies may face risk when payments, refunds, adjustments, or disbursements are tied to an identity that has not been properly verified.



Property title fraud: Bad actors can impersonate property owners, pay required recording fees, and file fraudulent deeds transferring or encumbering property.



Account creation and profile changes: A bad actor could create or take over a government service account, update contact information, redirect notices, or gain access to services before a payment is ever made.



High-value or sensitive transactions: Payments tied to regulated services, public records, business filings, or credentials may require stronger assurance because the downstream impact of serving the wrong person can be significant.

For government agencies, the practical implication is clear: Identity risk exists on both sides of the payment flow. Accepting a payment and disbursing a payment are different operating models, but both depend on the same underlying question: Is the right person or entity involved in the transaction?



Accepting payments: Trusting the person behind the payment

When agencies accept payments, card approval is only part of the risk assessment. The more strategic question is whether the person paying is authorized to access the service, record, license, permit, filing, account, or obligation associated with the transaction. A payment may clear successfully, but the agency still needs confidence that the person behind it is entitled to complete the action. Identity assurance turns payment acceptance from a narrow transaction check into a broader trust decision.

Disbursing payments: Identity assurance protects public funds

Disbursement creates a different but equally important trust challenge. When agencies issue refunds, benefits, grants, reimbursements, or other payments, they are releasing public funds. The risk lies in disbursing funds to an ineligible, fraudulent, or unverified recipient. Identity assurance helps agencies confirm that recipients are legitimate and eligible, reducing exposure to synthetic identities, compromised accounts, mule accounts, and other unauthorized individuals or entities.

In both acceptance and disbursement, payment approval alone is no longer enough. Agencies need greater confidence that the person initiating or receiving the transaction is the right person, acting for the right purpose, and with the right level of authorization. Identity should therefore be viewed not as a downstream fraud tool, but as a strategic layer of the payment ecosystem.

This does not mean adding friction to every interaction. The goal is to use identity intelligently: establish confidence earlier in the customer journey, apply additional verification when risk requires it, and preserve a seamless experience for trusted users.

Preparing for a future of automated fraud

As payment fraud becomes more sophisticated and AI-enabled, the payment industry must move beyond a narrow focus on whether a transaction can be approved. The more important question is whether payments should be approved.

Identity assurance, and the platforms that support it, help organizations reduce fraud losses, lower chargeback exposure, protect accounts at critical moments, and make smarter risk decisions without adding unnecessary friction for legitimate users. They also reinforce customer confidence by showing that identity is being protected with the same level of care as payment information.

ARTICLE

For government agencies, this shift is especially important. Payments are often tied to public records, licenses, permits, benefits, reimbursements, and other services where trust, eligibility, and authorization are critical. Bad actors increasingly target these services to defraud others. In these environments, payments linked to identity assurance platforms can help agencies protect public funds, preserve program integrity, strengthen service delivery, and ensure the right person or entity is served.

This is where the future of payments is headed. Done well, identity becomes more than a fraud-control mechanism. It becomes a trust infrastructure that supports security, service delivery, and the customer experience. The future of payments will not be defined solely by whether a card can be approved. It will be determined by whether organizations can trust the person behind the transaction.



For more information about our solutions,
please scan the QR Code or visit
<https://risk.lexisnexis.com/products/payment-solutions>



About LexisNexis Risk Solutions

LexisNexis® Risk Solutions includes seven brands that span multiple industries and sectors. We harness the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit risk.lexisnexis.com and www.relx.com.

Payment Solutions provided by LexisNexis is not provided by "consumer reporting agencies" as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("FCRA") and does not constitute a "consumer report" as that term is defined in the FCRA. Payment Solutions may not be used in whole or in part as a factor in determining eligibility for credit, insurance, or employment or for any other eligibility purpose that would qualify it as a consumer report under the FCRA. Due to the nature and origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies. © 2026 LexisNexis Risk Solutions. NXR17182-00-1026-EN-US