GRANULAR

Digital Commerce, Behavioural Data and Accountability

Public Education Edition

FilmPass & Co

Research period: 23 December 2024 - 23 December 2025

Education edition prepared 31 October 2026

Follow the event. Separate the records. Trace the connections. Ask what happens next.

Contents

Use a chapter link below to choose your starting point. Each page includes a return link to these contents.

Authorial Context - 3

0. Executive Orientation - 5

1. Positioning and the Boundary Lens - 7

2. Definitions and Guardrails - 11

3. The Ingredients List - 17

4. The Crumb Layer - 23

5. The Glue Layer - 29

6. The CUG Illusion - 37

7. Applied Mapping: Transaction-Level Reality - 43

8. Fraud Signals as a Possible Anchor Layer - 50

9. Governance Reality: Access and Accountability - 57

10. Value Creation vs Value Extraction - 63

11. What Good Looks Like - 73

12. Governance, Visibility and Responsibility - 79

Final Conclusion: Making the System Legible - 92

Final Reflection - 94

Public Technical and Regulatory References - 96

This paper distinguishes documented capabilities, illustrative mechanisms and evidence of actual use. Read the conditions attached to each explanation.

Authorial Context

FilmPass bought corporate cinema ticket stock from two suppliers it understood to be legally separate, for resale to members through benefit arrangements. FilmPass paused trading on 23 December 2024 while seeking answers about those purchases and the possible impact on members.

We understood the cinema tickets to be the product we were purchasing. We did not understand membership or use of a ticket to authorise undisclosed commercial uses of information about the people involved.

The effort to understand that experience prompted research into payment infrastructure, closed user groups, fulfilment, marketing systems and the information generated around a transaction. The original research period was 23 December 2024 to 23 December 2025. This public education edition was prepared on 31 October 2026.

The question is practical: when an organisation describes one part of a journey, what remains unexplained about the information collected, the connections made and the decisions that follow?

Granular examines possible mechanisms and the records needed to test them. It does not treat a company's description of its role as proof that it complied with its obligations. Nor does an unexplained outcome establish that a particular data transfer or misuse occurred.

Private correspondence, transaction schedules and proceedings are maintained separately. This paper supplies an educational framework rather than findings about the parties to those matters.

We continue to follow the relevant processes and will update our account when appropriate. Further research will be added as it is reviewed.

The purpose of this research

A consumer or small business should not need to reconstruct an entire technology stack merely to understand what happened to a purchase or to information about them. Yet a reply about one product can leave unanswered questions about another integration, recipient or later use.

The approach here is disciplined: identify the event, separate the records, trace each connection and ask who can explain the resulting decision. Technical capability matters, but capability is the beginning of an enquiry, not proof of execution.

The paper does not assume that closed user groups are ethical or privacy-preserving. Equally, it does not assume that every gated benefit programme behaves in the same way. The architecture, contracts, configuration, purposes and actual processing must be examined.

Three distinctions matter throughout: a documented product capability; an illustrative route that depends on stated assumptions; and evidence that a route actually operated. Those categories must not be collapsed into one another.

The central concern is whether the explanation given to a person covers what the assembled system actually does. A correct answer to a narrower question is not necessarily an adequate answer to the question asked.

A useful investigation does not end at 'read our policy'. It connects the policy to the relevant fields, dates, recipients, purposes and decisions.

0. Executive Orientation

0.1 What this paper examines

Granular studies the connections between commerce, payment, fraud-prevention, identity, marketing and benefit-fulfilment systems. Its focus is what can happen when information or observable outcomes are available across more than one context.

A customer can complete one checkout while several services create different records. An order record, an authentication exchange, a fraud assessment and a marketing event are not necessarily one shared payload. Their overlap must be established field by field.

The paper asks: what can each participant observe; what can it access or export; how can records be matched; and what later use or decision follows? A system's name does not settle these questions.

0.2 How to read the explanations

Worked routes are illustrative. They require the access, identifiers and integrations described. A supplier's product documentation can establish capability, but account permissions, deployment records and delivery logs are needed to establish operation in a particular case.

Descriptions of potentially lawful functions are not findings that any organisation complied with the law. Collection for one purpose does not give unlimited permission for another use.

0.3 The practical outcome

Use the explanations to turn a broad concern into a bounded question and a request for relevant records. Keep the distinction between what is confirmed, what is possible and what remains unexplained.

This is a public education paper, not a substitute for examining the evidence and legal rules applicable to an individual dispute.

0.4 The central research question

A purchase can create value beyond the product sold. Order frequency, redemption timing, membership eligibility and customer references can become commercially useful when they are accessible and connected. That does not mean all of those records are available to every participant.

The important boundary is between the purpose a person understands and the actual uses of information generated during the journey. A closed access gate does not describe downstream data permissions.

An organisation may have a limited role, but that role must be tested against its actual processing. Distributed systems do not remove accountability. Controllers and processors remain subject to the obligations that apply to their activities.

A technical flow may be poorly explained, incorrectly implemented or unlawfully reused. It may also have an explanation supported by records. Granular leaves those outcomes open to examination rather than deciding them from a provider's narrative.

Questions to carry through the paper

What was collected or generated? Which system created it? Who could access it? What crossed a boundary? Which identifier connected the records? Which purpose and authority applied? What subsequent decision relied on it?

A coherent answer links these stages. A policy, product label or statement that a tool is 'not for marketing' does not, by itself, describe every surrounding integration.

1. Positioning: How Granular Fits the Existing Body of Work

1.1 A synthesis of questions

Granular brings together questions about commerce, payments, identity, fraud prevention, membership, marketing and fulfilment. Looking at the components separately can leave the connections between them unexplained.

It does not assume that prior explanations were correct or that every apparent inconsistency has the same cause. It provides a method for comparing claims with relevant records.

1.2 Scope

The original research arose from FilmPass's experience. The public teaching routes use general explanations and hypothetical arrangements rather than reproducing private case files.

Public technical documentation can identify a possible capability. A policy can identify a stated purpose. A record can establish a particular event. A conclusion about actual conduct requires the appropriate combination of evidence.

The chapters that follow examine how to connect those sources without allowing one to stand in for another.

1.3 Look at the assembled journey

A typical teaching example contains a storefront, a checkout, payment and fraud services, analytics, a membership gate and fulfilment. Each has a different function. Actual deployments may combine or omit these components.

A component's stated role does not establish whether it collected only necessary information, acted only for that purpose or disclosed everything required. Those are questions for evidence and assessment.

1.4 Granular as a synthesis method

Read the explanations together, without assuming that every reply is either correct or incorrect. Ask what they cover, which records they describe and which question remains unanswered.

Useful enquiries include: can a result generated in a fraud assessment be seen by a merchant? Which result, rather than which raw telemetry? Can a merchant's own order history be joined to it? Is any later segmentation actually configured? What is the basis for that processing?

Information from several organisations may be needed to explain an end-to-end event. That practical difficulty does not excuse an incomplete response by an organisation responsible for particular personal information.

The method connects records and questions. It does not manufacture a shared profile from the fact that the same person visited several services.

1.5 The boundary lens

A boundary is a change in system, legal entity, purpose, access permission, identifier or decision-maker. At each boundary, record what moves and what does not.

For a proposed link, identify the source record, the receiving system and the field that connects them. Then establish whether the transfer or observation was possible, configured, delivered, received and used.

A common supplier, similar timestamp or repeated label can suggest a line of enquiry. None alone establishes a shared account, common controller, joined dataset or coordinated conduct.

1.6 Limited roles and incomplete answers

A payment provider may not run the storefront. A storefront may not determine a provider's fraud model. A benefit supplier may not process the payment. Such distinctions can be relevant without answering what each participant actually received or used.

Ask for the scope of the statement: 'Does that answer concern raw fraud telemetry, a visible risk result, our order data or a separate integration?'

Responsibility is assessed for the processing activity. It does not disappear because no single participant describes the complete journey.

This method helps a reader challenge a narrow answer precisely, without assuming the conclusion.

1.7 From a concern to a testable account

A person may experience an outcome that no single reply explains. The next step is to identify the relevant event, organisations and records, not to assume that a hidden complete profile exists.

An explanation can require several participants' records. A controller may also hold more information than its first response describes. Search scope, identifiers, access rights and actual holdings should be examined.

1.8 The role of prior research

Use a source for the claim it supports. A product document can show a capability. A policy can show what was declared. A dated record can show an event. Their combination may support an inference, which should remain identified as such.

1.9 Method in practice

Write down the proposed route. Mark each stage confirmed, possible or unresolved. Ask for the record that would resolve the first unsupported connection.

This approach can reveal an inadequate explanation without claiming that every part of the proposed mechanism has already been proved.

2. Definitions & Guardrails

2.1 Precision without unsupported assurances

The terms in this paper help readers distinguish formal roles from actual processing. A label in a contract or policy is evidence of what is stated; it is not conclusive proof of how a system operates.

2.2 Personal information and metadata

Personal information can include records and inferences relating to an identified or identifiable living person. Business activity does not automatically remove that character. A company as such is not a data subject, but an individual acting for it may be.

Metadata describes an event or record: for example a time, device characteristic, session identifier or processing status. A risk score, inferred preference or eligibility flag may also be personal information where it relates to an identifiable person.

Invoices, amounts and settlement records can contain personal information too. 'Metadata' is a descriptive category here, not a legal exemption or a claim that transactional information is excluded.

An inference can be stored in a field, calculated when needed or retained in another form. Whether a particular record exists, can be retrieved or must be disclosed requires examination of the processing and applicable rules.

A request should identify the person, relevant identifiers, period and categories sought. It should distinguish the individual placing an order, the cardholder and the eventual ticket user.

2.3 Business activity and access rights

A business purchase may involve several people: an employee using a browser, a cardholder whose card is charged and a member who redeems the ticket. Information about one is not automatically information about all of them.

An organisation should examine whose personal information it processes. A description such as 'business capacity' does not, by itself, answer an individual's request for personal information generated during that activity.

The right of access concerns personal information and supplementary information, subject to applicable restrictions and exemptions. It is not an unrestricted right to every business document, proprietary model or another person's information.

Ask which records were searched, which identifiers were used, which period was covered and whether any information was withheld. An organisation may need proportionate identification or clarification; that is different from dismissing an individual solely because the transaction was commercial.

2.4 Reading a fragmented response

A limited response can reflect a limited holding, an inadequate search, an exemption, an incorrectly framed request or another reason. The response and supporting records are needed to distinguish these possibilities.

The absence of a field from one disclosure does not prove that another organisation holds it. Conversely, a provider's narrow answer does not establish that no relevant personal information exists elsewhere in its systems.

The useful question is: 'Which personal information about this individual did you search for and disclose, and what explains the remaining categories?'

Source: ICO, What is the right of access? [3]

2.4 Fraud signals and their boundaries

Fraud tools may process transaction, device and activity information to assess risk. The fields and methods depend on the provider and implementation. A payment risk assessment is not automatically a general classification of a person's character.

Separate raw internal risk factors from results available to a merchant. A merchant-visible status, rule result or assessment does not establish access to all inputs that produced it.

A downstream system can only act on information or outcomes available to it. Timing, persistence and correlation alone do not demonstrate such access. Identify the report, interface, observation or independently collected record.

The purpose for collection and the purpose of later use are separate questions. A security justification does not automatically authorise commercial targeting. Actual processing requires assessment under the applicable rules.

Source: Stripe advanced fraud detection [2].

2.4 Closed User Groups

A closed user group restricts access to an offer or service by membership, eligibility or affiliation. It can involve an employer, customer community, student group or service organisation.

That definition concerns access. It does not establish whether information generated after access is shared, retained or reused, or whether those activities are justified.

A programme can include a portal, seller, payment service and fulfiller. Record the participants and purposes rather than assuming that the benefit's brand describes the complete arrangement.

The important distinction is between permission to obtain a benefit and the conditions governing the use of information around it. Those conditions require a separate explanation.

A person may be entitled to ask about information processed during their participation even where the purchase was made by an employer or business. Identify the individual and the relevant information.

The following section explains the roles of controllers, processors and joint controllers for those activities.

2.5 Roles and responsibility

Controllers determine the purposes and means of processing. Processors act on a controller's behalf. Joint controllership depends on the parties' actual involvement in determining purposes and means, not simply use of a common vendor.

A provider can have different roles for different activities. Examine the relevant operation rather than treating 'processor' or 'controller' as a permanent description of the whole organisation.

For a proposed route, identify who chose the purpose, who selected the data, who instructed the integration and who decided how the output would be used. Contracts, technical settings and actual practice can all matter.

2.6 Why precision matters

A statement about payment processing may not answer a question about independently controlled fraud information. A statement about raw telemetry may not answer a question about a merchant-visible assessment. A statement about anonymous totals may not cover a customer-linked export.

These distinctions do not establish wrongdoing. They identify the separate questions that need an answer.

The paper neither accepts nor rejects compliance merely because an organisation describes a bounded role. It asks whether that description fits the records and the processing at issue.

2.7 Section summary

Personal information can arise in business activity. Metadata and inferences are not automatically outside data-protection law. Fraud prevention, payment authentication, merchant reporting and marketing are distinct activities to examine.

A CUG's eligibility gate does not establish the permissions governing the information generated after entry. A provider's role must be assessed for the relevant processing.

Keep three levels separate: documented capability, illustrative mechanism and verified operation. A technical explanation is strongest when it states the conditions needed and the records that would confirm or rule out the proposed route.

The following sections use that discipline to examine fragmented events, connecting identifiers and downstream uses.

3. The Ingredients List

3.1 Identify components without assuming their configuration

A digital commerce journey can include a storefront, identity service, checkout, payment provider, fraud service, analytics, CRM and fulfilment provider. The presence of a tool name does not establish which features were enabled or what information it received.

3.2 Commerce platform

A storefront can hold orders, customer accounts and checkout references. Additional analytics, risk tools or extensions may also be configured. Do not assume that commerce software never classifies behaviour or that every installation does so.

For the event being examined, identify the platform, application version, installed integrations and relevant permissions. Separate the merchant's own collection from a provider's independently operated collection.

A session or account reference can support continuity within a system. To use it elsewhere, another system needs access and a reliable mapping.

The component list is a starting inventory. The configured flow is the evidence to examine.

3.3 Payment, authentication and risk

Payment processing, authentication and fraud assessment have related but different functions. Identify the provider and record for each operation.

A result may be retained after a transaction, but retention periods and later uses vary. Do not infer that every risk output persists indefinitely or follows a person across unrelated services.

Raw fraud telemetry can be held separately from merchant-visible payment records. A reporting interface may expose selected results without exposing the underlying observations.

3.4 Trust and review surfaces

Reviews, ratings and reassurance messages can influence a customer's decision. To establish that viewing or responding to them became a recorded signal, identify the collection mechanism and recipient.

The presence of a review widget does not itself show that a payment provider ingested review behaviour. A separate integration or collection route would need to be established.

Ask what the user saw, what was recorded and which system received that record.

3.5 Analytics and optimisation

An analytics service can analyse events it receives, such as page views, orders or conversions. A selected event may have several possible causes; it should not be treated as a reliable measure of personal intent without examination.

If analytics uses payment outcomes, identify how those outcomes arrive. It may receive a merchant-defined event rather than a provider's risk classification.

3.6 CRM and messaging

A CRM can store declared attributes, transaction history, calculated segments and inferred classifications. It is not limited to passive memory.

A connector can copy selected fields between systems where configured and authorised. Verify the actual field map, account scope, destination and delivery records. The connector's capabilities do not prove that a proposed transfer occurred.

A message or offer triggered by a record is a subsequent use to examine. Identify the rule, input and purpose rather than assuming that every customer communication derives from fraud data.

3.7 Eligibility and fulfilment

An eligibility service may return a yes/no result or more detailed information. A fulfilment service may record a ticket code, claim, delivery and redemption. Actual fields and retention differ between schemes.

Repeated use of an identifier can support a history within a service. It does not automatically prove that other services received that history.

A bulk stock purchase and individual redemption are separate events. A batch reference may connect the stock to the reseller without identifying every member. A claim mapping may create a person-level connection.

Ask whether the reporting available to each participant is aggregate, batch-level or individual. Then ask what further use is made of it.

An explanation of eligibility should not be substituted for an explanation of redemption reporting or later segmentation.

3.8 Coordination and visibility

A commercial arrangement may coordinate several brands or schemes. Establish the arrangement from relevant contracts, account relationships and actual configuration. A common vendor or similar interface does not prove common control.

Where one organisation operates several schemes, determine whether permissions separate their information. Shared infrastructure can support isolated tenants or controlled sharing; the architecture and settings decide the available routes.

3.9 The missing narrative

A person may need more than one participant's account to understand an event. This does not establish that no organisation holds a complete record or that the law cannot require relevant information.

The task is to identify who holds each part and which questions remain unanswered. A table of sources, recipients, fields and purposes is often more useful than a broad claim that the system is opaque.

3.10 Section summary

The components of a commerce journey may be familiar, while their connections remain difficult to see. Investigate those connections through configuration and event records.

For each component, distinguish stated purpose, actual data received, accessible outputs and subsequent use. Record the legal entity responsible for the relevant processing.

An integration's existence is not evidence that it transferred every available field. A successful payment is not evidence that every surrounding process was appropriate. A policy is not a complete execution log.

The following section examines the small records that can be created at these stages and the conditions under which they acquire wider meaning.

4. The Crumb Layer

4.1 Small records, larger questions

A journey can generate many separate pieces of information: a checkout event, an authentication result, an order reference, a redemption time or a customer-service outcome. Granular calls these fragments 'crumbs'.

A fragment may be innocuous in isolation yet informative when combined with other accessible records. That combination needs a demonstrable route and does not arise merely because several systems observe the same person.

4.2 Different origins

A storefront may record an order and campaign source. A payment provider may process transaction information and its own risk factors. A benefit platform may record eligibility and fulfilment. A marketing platform may receive a selected event through a configured integration.

These are possible categories, not a statement that every implementation collects or exchanges all of them. Identify the actual fields and recipients.

4.3 Purpose is a question, not an assurance

An operational explanation for a field does not settle necessity, proportionality, fairness or a later use. A fragment may itself be personal information, and a derived label can be personal information too.

The investigation begins with the record's origin and purpose. It follows what happens when that record is copied, transformed, combined or interpreted elsewhere.

4.4 Several routes can produce overlapping information

First, a provider may expose selected fields through a dashboard, API or report. Second, a merchant may independently collect an order event or session information. Third, an integration may receive an observable result such as success, challenge, refusal or redemption.

These routes are different. None establishes access to a provider's raw internal fraud telemetry. A reporting product's existence does not establish that a particular field is available.

4.5 What correlation requires

Matching records requires accessible information and a usable relationship: for example a customer key with a mapping, an order reference, or a combination of fields reliable enough for the intended use.

The same person visiting two unrelated systems does not cause them to exchange knowledge. A shared timestamp can suggest a candidate match but may collide, be rounded or reflect a different clock.

When a later system responds to an earlier outcome, identify how that outcome became observable. A redirect, receipt, webhook or common reference can provide a route; it must be established rather than assumed.

The absence of a bulk dataset transfer does not mean there was no disclosure or processing. Access to a result, repeated queries and independent overlapping collection are separate questions to test.

4.6 Risk information within a broader journey

Fraud services may use information across transactions to assess risk. A merchant's access to the resulting fields varies. Provider-internal processing and merchant-side reuse must be examined separately.

4.7 A profile needs a mechanism

A stored profile, a calculated segment and a decision generated on demand are different forms of processing. A distributed collection of events does not become a unified profile merely because it concerns the same person.

If several outcomes appear connected, identify the common input, feedback route or matching process. Other explanations, including independent rules or ordinary operational constraints, may also fit the events.

A technically possible route becomes persuasive when each connection is supported by records. Missing records leave a question; they do not automatically prove either absence or concealment.

4.8 Access requests and fragmented information

A subject access request can seek personal information held by the controller and the supplementary information required by law. It is not limited to facts typed into a form: relevant inferred or derived personal information can also fall within scope.

A response may cover only part of a journey. Whether it is complete, timely and lawful requires assessment of the request, information held, search and any applicable exemption. Fragmentation does not establish compliance or excuse an inadequate response.

4.9 Purpose limitation applies to inference

Creating or reusing a personal classification is processing. It does not escape purpose limitation because the information is inferred. Examine the purpose, compatibility of further processing where applicable, lawful basis, transparency and other relevant safeguards.

A security purpose is not a general permission to use the same information for commercial targeting. Equally, consent is not the only possible lawful basis for every operation. The precise activity and applicable rules matter.

4.10 Test the scope of an answer

'We do not share fraud data' should be tested against the data category and access method. Does the answer cover raw risk factors, a visible risk result, reports, exports and separately collected merchant information?

Ask what was accessible and what was actually used. Do not replace a vague denial with an equally broad allegation.

Sources: ICO access and purpose guidance [3,4]; Stripe advanced fraud detection [2].

4.10 Continued: one answer can leave another question open

A provider may accurately describe one operation while leaving a different operation unexplained. That is a reason to specify the unresolved question, not to assume that either every answer or every concern is correct.

For example: 'I understand that the fraud model is not a marketing tool. Which fields from this transaction, including any merchant-visible assessment, were available to reports or integrations, and which were delivered to another system?'

4.11 Follow the meaning as well as the field

An order status can become a segment label. A reversal count can become an inference about reliability. A member reference can become a customer join key. Each transformation needs its own explanation.

The field mapping, destination schema and rule using the result may reveal a change of context that a general policy does not explain.

A technical possibility remains an investigative question until the configured route and use are established. If the relevant field was never exposed or delivered, that may rule out the proposed route.

4.12 Section summary

Small event records can acquire wider meaning when they are accessible, linked and used. The record's origin does not settle the lawfulness of every subsequent use.

A clear explanation identifies the source, the recipient, the connecting field, any transformation and the decision that follows. Where context is lost, identify where it was omitted and whether the later inference is justified.

The absence of a bulk transfer is not the same as the absence of processing. But a joined profile cannot be inferred solely from shared infrastructure, timing or similar outcomes.

The next section examines the identifiers and mappings that can connect records - and the evidence needed to distinguish a real connection from coincidence.

5. The Glue Layer

5.1 What can connect records?

An order reference, customer key, payment reference, membership identifier or ticket code may connect stages of a journey. A connection requires the relevant values and mapping to be available to the system performing it.

A timestamp, amount or device characteristic may narrow candidates but may not uniquely identify a person or transaction. Collisions, shared devices and different clocks can create false matches.

5.2 Pseudonymous identifiers

A record without a name can still relate to an identifiable person where it can be connected using available information. Pseudonymisation is not automatically anonymisation.

Conversely, possession of a pseudonymous value does not prove that every recipient can identify its subject. Examine the additional information, access and realistic means of connection.

The useful question is: 'What can this recipient identify or infer from this field and the other information available to it?'

5.3 Follow the mapping

A key can change between systems. An integration may translate a storefront customer ID into a CRM contact ID, or connect an order to a payment reference. That mapping is often more informative than the label attached to either field.

Identify where the mapping is held, who can use it and whether it applies across accounts or schemes. A reused field name does not establish that values share a namespace.

5.4 Policy and configuration

A policy can describe a purpose or recipient category without listing every implementation detail. Compare it with the actual processing to assess whether the explanation is adequate.

Do not infer a technical relationship from an omission alone. Ask which records and integrations account for the event, and what information was given to the people concerned.

An identifiable gap is a basis for a precise follow-up question.

5.5 Access and supply can be different relationships

An employee may access a benefit through a membership portal while an SME buys stock under a separate supply arrangement. The same branding does not make those contracts, users or data flows identical.

Record who purchases, who pays, who receives the ticket and who redeems it. Trace any mapping between those roles.

5.6 Derived information

A system can calculate an attribute from records it holds or receives. Whether it stores the result, recalculates it later or deletes it depends on implementation.

A derived result does not become exempt from data-protection requirements simply because it is not a copy of the source record. If it relates to an identifiable person, examine its purpose, accuracy, disclosure and retention.

Ask both for the result and for enough information to understand its subject and use, within the applicable rights and limits.

5.7 Persistence and correction

Deleting one record does not necessarily remove every copy or derived result. It also does not mean those results persist forever. Establish the actual retention and deletion process.

Where an underlying event is corrected, identify which recipients and derived attributes need review. A recipient may retain the corrected source, an outdated copy or a different record entirely.

5.8 Boundary lens applied

The boundary is between a technical identifier and the meaning assigned to it. A match may identify an account without identifying the person who used it. An outcome may concern a merchant without describing customer misconduct.

Request the mapping and interpretation that support the conclusion. A supported correction should address both the original record and the later use that depended on it.

5.9 Section summary

Identifiers can connect records when the receiving system has both access and a usable mapping. Removing a name does not necessarily make a record anonymous. Conversely, two records about the same person are not automatically joined.

5.10 Identity stitching: establish the route

Identity stitching means associating records with the same person or account. It may use a common identifier, a mapped pair of identifiers or a probabilistic method. Each has different accuracy and access requirements.

Independent systems can observe overlapping events without exchanging their complete datasets. To conclude that one system learned from another, identify an observable output, shared reference, feedback route or other demonstrable connection.

The same human traversing several systems is not sufficient evidence of a unified profile. Common vendors and similar timestamps do not establish one either.

Ask for the match key, scope, confidence, mapping version and destination record. Determine whether the match describes a person, account, card, device, household or order; those subjects are not interchangeable.

A false match can be as consequential as an undisclosed correct match. Precision matters before any conclusion about the resulting profile.

5.11 Illustrative map: records and connecting evidence

Commerce layer

Possible records include an order reference, customer account and checkout events. A connection to a payment requires the associated payment reference or another verified mapping.

Payment and risk layer

Possible records include the payment status and any assessment exposed to an authorised user. These must be distinguished from raw internal risk factors that may not be available to the merchant.

Benefit and fulfilment layer

Possible records include a ticket code, claim reference, redemption time and outcome. A connection to the purchaser requires a mapping from stock or batch to an individual claim.

Marketing or CRM layer

A configured integration may import selected events and identifiers. Establish its field list, permissions, delivery record and the rule that uses the imported information.

The connection test

For every arrow, name what crossed the boundary. If it was an observable result rather than a copied dataset, state that clearly. If it was independently collected data, identify its separate source.

An empty arrow is an unanswered question. A diagram must not turn it into a proven transfer.

5.12 What a connected record can reveal

When available records are reliably matched, a recipient may infer frequency, preferences, conversion patterns or eligibility. Those are possible uses of a configured system, not inevitable consequences of taking a payment.

An inference should retain its source, date, subject and uncertainty. A merchant's refund count, a cardholder's authentication outcome and a member's redemption history describe different events and potentially different people.

5.13 Reading denials precisely

An organisation may not share raw datasets yet expose selected results. Another may collect similar information independently. A third may have no access to either route. Distinguish these cases before interpreting a statement that information is 'not shared'.

No single answer establishes all routes. Ask the provider to address the specific field, access method, recipient and period at issue.

5.14 Boundary lens applied

The boundary is between an available record and a supported conclusion. A technical join can be possible without being used; a completed join can exist without establishing a lawful purpose; a lawfully obtained result can still be interpreted inaccurately.

Those are distinct questions, and each needs a record rather than an assumption.

5.15 Boundary lens: separation and connection

Separate legal entities may share selected information under an arrangement, use the same service without sharing it, or independently observe related events. These are different situations.

A claim of separation should be tested against actual access and processing. A claim of connection should be tested against the route and records supporting it.

For the reader, the practical safeguard is precision. Identify the subject, source, identifier, recipient and use. Record where the evidence ends.

The next chapter applies this method to closed user groups, where confidence in an eligibility gate can be mistaken for an explanation of the entire information journey.

6. The CUG Illusion

Access control is not a complete explanation of data use

6.1 Purpose of this section

A closed user group restricts eligibility for an offer or service. It may serve employees, students, customers, key workers, police or armed-forces communities. 'Closed' describes admission; it does not, by itself, describe every system and recipient involved after entry.

The concern is the expectation created by an exclusive or trusted benefit. A person may understand that eligibility is checked without understanding the information generated during purchase, authentication, redemption or later marketing.

6.2 The questions behind the benefit

Who verifies membership? What proof is retained? Which supplier fulfils the offer? Who receives reports? Is a person's membership connected to shopping history? Are results used for another commercial purpose?

A gated scheme is not inherently ethical or compliant. Nor does a common service provider prove that separate merchants pool their customer information. The actual architecture and uses need examination.

This chapter examines the risks that can arise when the explanation stops at the gate while the information journey continues beyond it.

6.3 A benefit can involve several organisations

The membership portal, ticket seller, payment service and fulfilment provider may be different entities. A single branded experience can conceal this complexity from a reader without proving that anyone deliberately concealed it.

At each stage, identify the legal entity, role, data received and purpose. Do not infer a shared database merely because services use the same platform.

6.4 The employer's perimeter and the member's journey

An employer's internal security does not describe a member's interaction with an external benefit website. The member may leave the employer's systems and transact with separately operated services.

That is a reason to examine vendor selection, privacy information, access controls and incident handling. It is not evidence that the employer's network has been breached or that every benefit supplier can see employment records.

6.5 Trust and disclosure

Employer endorsement can influence a member's confidence. The operational explanation should therefore make the external participants and their uses understandable at the relevant point in the journey.

An attractive benefit does not answer whether the person understood the additional processing around it.

6.6 Employee and customer exposure

A membership category can provide context about a person. An eligibility check may confirm only a yes/no result, or it may involve more detailed evidence. Those implementations create different exposure and retention questions.

Ask whether the supplier receives a category, an identifier, a document or merely an authorisation token. Ask what is retained and whether it is associated with order or redemption history.

6.7 Separate purchase, member and beneficiary

An employer can buy stock in bulk, an administrator can pay and a member can redeem later. A bulk purchase does not automatically identify every beneficiary. A mapping, claim or registration step may establish that connection.

Where such a mapping exists, the supplier may learn more about the SME's customer relationships than the bulk invoice alone would reveal. The commercial significance depends on the fields available and their actual use.

6.8 The transparency question

Does the explanation cover eligibility only, or also purchase reporting, redemption, segmentation and any further commercial use? The member should be able to identify who can answer those distinct questions.

A closed access gate does not itself constrain telemetry, reports or integrations. Those require their own controls.

6.9 Commercial incentives and unequal visibility

A benefit programme can generate commercial information about conversion, frequency, product choice or redemption. Which organisation benefits from those insights depends on the reporting arrangements, identifiers and permitted uses.

The concern is an imbalance: a small business may carry the customer relationship while a supplier sees a broader pattern through fulfilment or reporting. Establish that visibility rather than assuming every intermediary has it.

6.10 Key workers and service communities

Where a scheme relates to police, armed forces, healthcare or other service communities, the membership context can make unwanted identification or targeting particularly consequential.

This is a reason for careful minimisation, access and retention decisions. It is not a claim that all occupational data is special-category data, that every scheme holds sensitive operational details or that a national-security incident has occurred.

6.11 Questions for organisations offering benefits

Which fields reveal affiliation? Is detailed proof necessary or would a limited eligibility result suffice? Who can view that information? Can it be linked to purchases? What happens when employment or membership ends?

A security assessment should follow the actual information and recipients. The word 'exclusive' is not an assessment.

6.12 The CUG reality test

Can the member identify the seller, fulfilment provider and relevant controllers? Can they understand which information each receives? Can they distinguish delivery of the benefit from analytics, targeting and further reuse?

Can the organisation offering the scheme explain the supplier's reporting access and onward integrations? Are there limits on customer-level reporting? Can errors and deletion requests reach the relevant copies?

6.13 Trust does not replace verification

Single sign-on and tokenised links can simplify access. They do not settle downstream purposes or the trustworthiness of every later message. A token's scope and expiry should be understood separately from the member's broader account.

6.14 Boundary lens applied

Admission is one control. Information use requires further controls. A system can be closed to non-members while involving external processing; whether that processing is justified and transparent depends on the actual arrangement.

The useful challenge is: 'Please show how the protections described at entry continue through purchase, redemption, reporting and subsequent use.'

6.15 Section summary

CUGs can concentrate a defined audience and the trust associated with a benefit. That creates questions about commercial incentives and information use; it is not an endorsement of the model.

The key distinction is between permission to receive a benefit and the lawful conditions for processing information generated around it. One does not automatically establish the other.

A reader should leave this chapter asking who can connect membership, purchases and redemption; who benefits from that connection; and how the member can see or challenge the resulting use.

The next section follows the purchase surface, contractual seller and payment attribution. These can differ, but their relationship should be explainable from relevant records.

7. Applied Mapping: Transaction-Level Reality

7.1 Begin with the purchase

Record the website used, the seller identified at the time, the order reference, amount and product. Keep these separate from a bank statement descriptor and a payment provider's merchant-account identity.

A descriptor can be abbreviated or use a trading name. It does not necessarily identify every entity involved. A mismatch should prompt an explanation tied to the actual transaction.

7.2 A fictional voucher example

A buyer purchases ticket stock on Website A. Its terms identify Supplier B. The payment is recorded under a descriptor that the buyer associates with Brand C. A different service handles redemption.

This example identifies questions, not a finding of misrepresentation. Who contracted to supply the stock? Which entity received the payment? What explains the descriptor? Who fulfilled the ticket? Which controller processed each category of personal information?

The supporting records should connect those answers to the transaction date.

7.2 Continued: map the references

Order to payment

Use the order reference and associated payment or receipt identifier. A matching amount and date can support a search but may not uniquely establish the connection.

Payment to merchant

Ask for the merchant identity relevant to the payment and the explanation for the displayed descriptor. Distinguish the account holder, payment service, connected account and any platform arrangement.

Stock to redemption

Identify whether the ticket or batch code connects the supplier's stock to the reseller, an individual member or both. A bulk invoice alone may not contain the member-level mapping.

Historical changes

If a website, name or route changed, use dated records to establish what changed and when. A later record should not silently overwrite the explanation of an earlier transaction.

The diagram or chronology should mark an unverified connection as unresolved.

7.3 Align the entities before drawing a conclusion

In a fictional voucher purchase, the customer may see a branded website, contract with a benefits supplier and see a different descriptor on a bank statement. A payment processor may hold a merchant-account identity that requires explanation alongside those records.

Record each legal entity and its role at the transaction date. A trading name, processor account, supplier relationship and corporate parent are different concepts. A mismatch is a question to resolve, not automatic proof of misdirection or common ownership.

7.4 Seek a transaction-specific explanation

Ask how the order reference connects to the payment reference, merchant identity and fulfilment record. Where the requested information concerns another party, the provider may need to consider confidentiality, rights and applicable disclosure routes.

A statement that a court order is needed should be examined for its scope and basis. It does not establish that every question requires court proceedings or that regulators lack investigative powers.

7.5 Follow the three layers

Purchase surface: where the customer placed the order. Contractual relationship: who sold the product and on what terms. Processing and fulfilment: who handled payment, information and delivery.

A supported explanation reconnects those layers without substituting a current brand name for the relevant historical entity.

7.6 The three perspectives

The buyer sees the purchase interface and representations. The payment system holds transaction and merchant references. The fulfilment system records delivery or redemption. Their records may use different identifiers.

A reconciliation should show how those identifiers correspond. It should not assume that every discrepancy is wrongful or that every difference is harmless.

7.7 Why a reply can miss the question

A response explaining a legitimate supplier relationship may still leave unanswered who sold this buyer the stock or which entity processed the buyer's information.

Restate the question using the specific transaction and requested distinction: seller, beneficiary, account holder, controller or fulfiller. Avoid asking one broad term to stand for all of them.

7.8 Redemption as a separate event

Entering a ticket code can create a record of an attempted or completed redemption. The fields might include the code, time, venue and result, depending on the system.

That record can help establish fulfilment. It does not automatically establish the identity, motivation or reliability of the person using the ticket. The purchaser and user may be different people.

Ask whether the redemption is linked to the original stock purchase, a member account or another reference. Ask which participants can view the resulting history and what reporting or segmentation uses it.

A successful redemption may be useful information; a failed attempt may require explanation. Neither should be promoted into a general personal judgement without an adequate basis.

Keep the commercial allocation of responsibility separate from the technical record. Who handles a complaint and who controls the relevant information may differ.

7.9 Section conclusion

An end-to-end account may require purchase, payment, fulfilment and privacy records. The number of organisations involved does not determine the answer in advance.

Keep legal identity, customer-facing brand, payment reference and controller role distinct. Then show the connections supported by dated documents.

The purpose of this method is to obtain an intelligible explanation. It does not certify a discrepancy as compliant or convert it automatically into proof of misconduct.

The next section examines risk information and the questions that arise when a result is retained, exposed or interpreted in another context.

Worked example: reconcile a ticket journey

An SME buys a fictional batch of 100 tickets. A supplier holds the invoice and batch reference. A member later claims one ticket through a benefit portal.

Question 1: Does the portal record which member received which code?

Question 2: Can the supplier connect that code to the batch and the SME?

Question 3: Does redemption reporting identify the member or only the code?

Question 4: Does any participant use that mapping for a purpose beyond fulfilment or support?

The first two connections might be present while the third is absent. A batch-level record does not automatically reveal the member. Conversely, removing the member's name from an export does not necessarily break the connection if an accessible mapping remains.

List each connection as confirmed, unresolved or absent. Then ask for the next relevant record.

This is an invented teaching example; the numbers are not a transaction schedule.

8. Fraud Signals as a Possible Anchor Layer

8.1 Scope of the question

Fraud services can process information about transactions, devices and activity to assess risk. Some systems use patterns across events. Their actual inputs, retention and exposed outputs vary.

The research question is whether a result or overlapping record becomes available to another activity, and how it is then interpreted. The existence of a fraud service does not answer that question.

8.2 Raw factors, results and merchant records

Raw provider-internal risk factors are not the same as a merchant-visible assessment. A merchant's order history is not automatically a fraud dataset. A separately installed analytics script has its own collection route.

Trace each category to its source. Establish the fields the recipient could access and the fields it actually received.

A claim that a tool is not a marketing product does not explain every surrounding integration. But its raw inputs cannot be assumed exportable merely because a reporting tool exists.

8.3 Persistence needs evidence

A risk-related record may remain after a transaction for a stated purpose and retention period. Determine which record, whose information it concerns and how it is later used.

A stored dispute history, a model output and a merchant account balance are different records. The disappearance of one does not establish the presence or absence of the others.

8.4 Downstream meaning

A result created for one decision may be inappropriate for another. An assessment of transaction risk should not automatically be treated as a reliable judgement about a member's character or entitlement.

If another system uses the result, identify its input, rule, purpose and review process. If the route cannot be established, retain it as an investigative hypothesis.

This preserves the central concern about reuse without inventing access, permanence or consequences.

8.5 Illustrative pause and chargeback context

Consider a fictional merchant that pauses fulfilment while investigating supply concerns. Some customers seek refunds or chargebacks. The existence of those events does not, by itself, establish customer fraud.

A record may describe a dispute against the merchant, an account balance or a card transaction. Identify its subject before interpreting it as a judgement about the customer.

8.6 What can survive resolution?

A closed financial dispute does not necessarily delete every related record. Retention and use depend on the provider, purpose and applicable requirements. A downstream system may preserve detailed reasons, or a selected export may omit them.

The relevant question is whether the source context reached the recipient and whether the recipient's rule interpreted it correctly. It is inaccurate to assume that all fraud systems discard the justification for a reversal.

Ask for the dispute reason, outcome, subject, retained fields, destination mapping and any later decision. A reversal count alone is not a finding of dishonesty.

If a customer-linked label remains after correction, ask how the original correction propagates to derived records and recipients.

8.7 Outcomes can influence another system only through a route

A later service may observe a successful checkout, a challenge or an abandoned purchase. Establish how it receives or detects that outcome: a merchant-defined event, API response, redirect or another mechanism.

The observation may reveal that a journey stopped without revealing why. It should not automatically be interpreted as fraud or personal unreliability.

8.8 Marketing and access decisions

A marketing platform may receive conversion events from a configured integration. That does not prove that it receives the payment provider's fraud data. The event definition, fields and source are essential.

If a price, offer or eligibility decision is alleged to depend on a risk-related result, obtain the actual decision rule and connecting record where available. A commercial effect cannot be inferred from the presence of analytics alone.

The concern is legitimate to investigate: an outcome collected in one setting may influence another. The route and interpretation must still be established.

8.10 Access and commercial advantage

A participant with more complete reporting may understand patterns that another cannot see. Whether that advantage exists depends on the actual information and permissions, not simply the participant's size or position.

8.11 Trace any consequence

A payment risk assessment, a merchant segment, a fraud-database marker and an insurance record are separate systems. A consequence in another sector requires evidence that relevant information reached and influenced that decision.

Do not infer a banking, insurance or employment effect solely from a payment refusal. Ask for the actual decision, information relied upon and responsible organisation.

Where a connection is established, examine whether the information was accurate, appropriately interpreted and used for a justified purpose. Where it is not established, the concern remains a question rather than a confirmed consequence.

8.12 Worked routes from a result to another use

Visible assessment to CRM

Assumption: an authorised merchant can access a particular assessment and a configured integration imports it with a customer reference. Check field availability, permissions, delivery and the CRM rule. This does not imply access to raw internal risk factors.

Independent collection

Assumption: a merchant separately records checkout activity and order history. A later segment can use those merchant records without receiving the payment provider's raw telemetry. Identify that independent source rather than attributing every field to fraud prevention.

Outcome observation

Assumption: a recipient observes success, challenge, refusal or redemption and uses it as feedback. Establish the route and interpretation. An observed outcome may reflect many causes and should not automatically become a label about personal reliability.

8.13 Section conclusion

The research question is whether an accessible record or result changes purpose or meaning downstream. That route must be supported by fields, mappings and use. A shared person or infrastructure is not enough to prove it.

The legal assessment is separate: obtaining information does not establish permission for every later use, and an inferred personal classification remains subject to applicable data-protection requirements.

Sources: Stripe advanced fraud detection [2]; ICO purpose and access guidance [3,4].

Worked example: the reversal with two meanings

A fictional customer receives a refund because the supplier cancelled an order. The source record includes the cancellation reason. An export contains only customer reference, amount and reversal count.

A later rule treats repeated reversals as customer abuse. In this scenario the error is in the omitted context and the rule's interpretation, not in the customer's request for a refund.

Ask which reason fields existed, which were exported, which person the record described and which rule produced the restriction. A correction should address the dependent label as well as the source event.

A different implementation may preserve the full reason and review it correctly. The example identifies what to test; it does not claim that all payment or fraud services discard context.

The lesson is that a financially resolved event can still need a data explanation if another decision relies on its record.

9. Governance Reality: Access and Accountability

9.1 The problem to examine

A fragmented system can make it difficult to obtain a clear explanation. That does not establish that its participants complied with their duties or that the law has no application to the combined activities.

9.2 Match the request to the issue

A refund request, a merchant-identification question, a subject access request and a complaint about personal-data use are different requests. An answer to one may leave another unresolved.

State the activity, person, period and information at issue. Keep a short record of what was requested, what was answered and what remains missing.

The objective is to connect the operational question with the relevant duty and responsible organisation. A broad policy response should be assessed against the question actually asked.

9.3 Transparency across a connected system

Data-protection duties are not confined to simple linear databases. Controllers must address their processing of personal information, including relevant derived information, recipients and purposes. Distributed architecture can make investigation harder without displacing those duties.

9.4 Records and decisions

A data issue can concern loss of a record, an inaccurate classification or an unexplained use. These are different problems. Identifying a state change in a system is not evidence that the state is outside the law or that no disclosable information exists.

Ask what information was used to create a result, what the result means and who relied on it. Where a model or business logic cannot be disclosed in full, that does not settle every question about the person's information and the explanation required.

9.5 Fragmented responses

A response from one organisation may not describe another organisation's processing. It may also be incomplete for reasons that require investigation. Do not certify a response as compliant simply because it concerns one part of the journey.

A practical record separates the request, scope searched, information supplied, stated exclusions and remaining questions. That makes it possible to challenge the actual gap rather than argue about labels.

9.6 Business capacity and personal information

A company has no individual subject-access right merely as a company. An identifiable person may nevertheless generate personal information while acting for that company.

A refusal based on 'business capacity' therefore needs examination of the particular information, the person's relationship to it and any relevant exemption. It should not be treated as an automatic exclusion of behavioural or technical information.

Controller and processor roles also need examination for the specific activity. A processor-only description of one service does not establish the role for every separate operation.

9.7 Voucher redemption as a point of connection

A ticket can be purchased in bulk and redeemed later by a different person. A redemption system might record a code, time, venue and outcome. Whether that becomes linked to the purchaser or member depends on the mappings and identifiers actually held.

Ask whether reporting is aggregate, batch-level or person-level. Ask who can access it and whether it is used only for fulfilment or also for another purpose.

The question is not whether a ticket necessarily creates a wider profile. It is whether the particular arrangement permits or performs that connection, and how it is explained.

9.8 A label does not settle the processing

Terms such as 'operational', 'aggregated', 'anonymous' or 'business data' require context. Ask what the field contains, whom it relates to and what additional information can connect it to a person.

9.9 Documentation and practice

Policies and contracts describe intended activities and responsibilities. They should be compared with actual configuration, records and use. Their existence alone does not establish compliance.

9.10 A usable account

An explanation should identify the source, purpose, recipients, retention and relevant decisions. Where a request is limited or refused, examine the reason and the applicable right or exemption.

A privacy notice is not an execution log, but technical complexity does not remove transparency obligations.

9.11 Following the relevant process

An organisation's complaint route, an individual's information rights, regulatory powers and court procedures have different purposes and limits. Use the route appropriate to the question rather than treating them as interchangeable.

9.12 Investigating a connected flow

A regulator may investigate relevant processing and use its statutory powers. A court may order disclosure within applicable proceedings. Controllers may provide information or coordinate responses without either step.

A complaint should distinguish the supported facts from the proposed mechanism and identify the information needed to resolve it. This helps a reviewer assess the gap without requiring acceptance of every wider concern.

Fragmentation can make a case harder to explain. It does not establish that no reviewer can examine the connected activities.

9.13 Routes to information

Court procedures may provide relevant disclosure, subject to their rules and scope. They are not the only possible route. Controllers can cooperate, individuals can exercise information rights, and regulators have investigative and enforcement powers.

None of these routes guarantees access to every internal document. Identify the information sought and the purpose of the request, rather than assuming a blanket entitlement or a blanket prohibition.

9.14 Boundary lens applied

The boundary is between a formal response and an adequately explained activity. A response should be tested against the relevant obligations; it is neither automatically compliant nor automatically defective because other organisations are involved.

9.15 Section conclusion

Fragmentation is an investigative problem, not a legal exemption. Inferences and linked records can still be personal information. Roles, purposes and responsibilities must be assessed for the actual processing.

The useful next step is a precise request supported by an event, identifier, period and unresolved question. Where a response remains inadequate, use the available complaint, regulatory or legal route appropriate to the issue.

Sources: ICO right of access [3] and enforcement guidance [5].

10. Value Creation vs Value Extraction

10.1 What can make information commercially useful?

Context can improve a decision: what was bought, when, how frequently and whether the benefit was used. A supplier or intermediary with access to connected records may see patterns that a participant with fewer records cannot.

That potential creates an incentive to collect, connect or retain information. It does not establish that a particular organisation did so or that the resulting analysis is accurate.

10.2 Authentication is not a universal historical explanation

Richer authentication context is part of the technical background, but it does not prove that CUG business models changed for one reason or at one date. Marketing, analytics and member reporting existed before 3DS2.

Investigate deployment and integration changes using contemporaneous records. Separate authentication, payment authorisation, fraud assessment and marketing use.

The commercial question is who can use the information, for what decision and with what benefit or risk to the people and businesses involved.

10.2 Who can see across contexts?

An intermediary may have information from several schemes. Whether it can link the same person across them depends on identifiers, access controls and actual processing. Being positioned between organisations is not enough on its own.

10.3 Who benefits from the resulting insight?

A connected record may support reporting, planning, segmentation or targeting. Establish which decision it supports, which organisation uses it and what value or risk follows.

An SME may have less visibility than a fulfiller into member-level redemption, while having more visibility into its own customer relationship. Compare actual access rather than assuming one participant has the complete picture.

A wider view can create commercial incentives to seek or retain information. That incentive is a reason for scrutiny, not proof that a particular use occurred.

10.4 Membership and commercial information

A defined audience may be attractive to brands because of its eligibility, interests or purchasing context. That commercial appeal does not establish what personal information a particular programme collects or shares.

10.5 Ask what the supplier can learn

Can it see aggregate demand, the SME's purchase pattern, individual claims or identified member activity? Which of those records can it connect across schemes?

Those levels of visibility are different. Ask for reporting fields and access scope rather than assuming that every supplier has a complete customer profile.

10.6 Value beyond the ticket

A transaction can inform demand planning, offer selection or a later campaign where suitable records are available. The relevant use needs its own assessment of purpose, accuracy, transparency and authority.

A benefit price does not explain that use. Nor does a potential commercial advantage prove that it occurred.

10.7 What redemption can and cannot establish

A redemption record may confirm that a ticket or code was used in a particular system. It can contribute to fulfilment accounting and reporting.

It does not automatically confirm who used the ticket, why they used it, whether they were satisfied or whether they are generally reliable. A transferred ticket, shared account or incomplete mapping may change the interpretation.

A failed redemption also has several possible explanations: expiry, an invalid code, a system fault, venue restrictions or another issue. The record and context are needed.

10.7.1 Questions about reporting

Which participant receives the result? Is reporting aggregate or linked to a person? How long is it retained? Is it used to deliver the benefit, improve the service or support a different commercial activity?

Treat redemption as an observed event, not a universal measure of personal reliability.

10.8 Voucher categories and information use

Tax treatment and data processing are separate questions. Do not infer a voucher's legal tax classification solely from the existence of a choice at redemption or from a particular data flow.

If tax classification matters, examine the applicable rules and the voucher's terms, supply and tax treatment at issue. A technical explanation of redemption is not a tax determination.

For this paper, the important point is that purchase and redemption can generate different records at different times. Those records may be linked, but the mapping must be established.

Ask which information becomes available only at redemption and who can use it. That question remains useful without alleging that the voucher was classified incorrectly.

10.8 Context and allocation of risk

An event can have different significance for different participants. A chargeback may concern non-delivery, a disputed authorisation or another reason. A failed redemption may concern an expired code, a system fault or eligibility.

The record should preserve enough context for the relevant use. Whether a particular export omitted that context requires inspection of the source and destination fields.

Where an SME faces a loss or restriction, identify the decision and its basis. Do not assume that every adverse outcome was caused by a hidden profile.

A precise account can still be critical: if an organisation relies on an incomplete label, ask it to explain and review that reliance.

10.9 Compare incentives using the actual arrangement

A supplier might benefit from accurate fulfilment reporting. A marketer might value information about repeat use. An SME might need to resolve a member's failed redemption. These interests can overlap without being identical.

Do not assign a universal level of tracking, liability or commercial value to a voucher category. Examine the contract, reporting arrangement and actual processing.

A useful comparison records: the decision supported; the information used; the person or business affected; the organisation benefiting; and the explanation provided.

If a later use is poorly explained, ask for its purpose and basis. If it is not performed, do not attribute it merely because the information would be commercially useful.

10.10 Completion and explanation

A system may prioritise a smooth customer journey while making its information processing difficult to understand. That is a design question to examine, not proof that explainability is impossible.

The commercial incentives to reduce friction and improve conversion should be considered alongside transparency, minimisation, accuracy and accountability.

10.11 Who carries the consequences?

A member may experience the restriction. An SME may handle the complaint. A supplier may hold the relevant record. Map these responsibilities rather than assuming that the customer-facing party controls every decision.

A provider's legitimate purpose does not settle another participant's use, and the architecture alone does not establish that everyone acted correctly.

The next chapter asks what a clear and accountable arrangement should make visible.

10.12 Purchase and redemption describe different events

A purchase record can show acquisition of stock or a ticket. A redemption record can show use of a code. Neither automatically describes the same person, and neither alone establishes personal reliability.

The connection between them may be an order reference, batch mapping or individual claim record. Verify which connection exists.

The meaning of a delay or failure also depends on context. A member may choose a later visit, encounter an unavailable screening or receive a replacement ticket. An isolated timing field may not distinguish those causes.

10.13 Boundary lens applied

The boundary is between an observed event and an inferred attribute. Ask what evidence supports the inference and whether the uncertainty is retained when the result travels onward.

10.14 Section conclusion

Linked information can have commercial value. That value is not a universal price per profile and cannot be established from a product label alone.

The meaningful questions are what information is available, which connections are made, who uses the result and how that use affects members and SMEs.

CUGs concentrate an eligible audience. Whether they also concentrate linked customer knowledge depends on the actual systems and permissions. That distinction should be explained rather than assumed.

The next section sets out practical characteristics of an accountable arrangement. It does not certify current providers as meeting them.

11. What Good Looks Like

11.1 An assessment framework

This section describes questions and safeguards for evaluating an arrangement. It does not conclude that existing systems need no restriction or that their current practices are acceptable.

11.2 Clear roles at the relevant point

Identify the seller, fulfilment provider and controllers for the processing concerned. Distinguish the benefit's brand from the legal entities behind it.

Explain when the user moves to another service and which information is passed or separately collected. A single visual brand should not substitute for the operational explanation.

11.3 Honest CUG framing

Describe what the eligibility gate controls and what it does not. Make reporting, retention and any subsequent use understandable rather than relying on the reassuring word 'closed'.

A suitable arrangement should support informed questions, accurate records and effective correction. Its actual performance must be assessed against those expectations.

11.4 Explain fraud processing and any later use

Fraud prevention serves an important purpose. That does not establish that every collection or subsequent use is necessary, proportionate or otherwise lawful.

An explanation should distinguish the protective activity from any later reporting, profiling or commercial use. Identify which outputs are available to whom and which are retained internally.

11.5 Make eligibility and fulfilment understandable

Explain who verifies access, who sells and supplies the ticket, and who can see redemption. A member should not need to infer these roles from unrelated documents.

11.6 Consider the membership context

Affiliation with an employer or service community can make unwanted identification consequential. Use limited verification where appropriate, restrict access and examine retention.

Do not assume every occupational category is legally special-category information. Assess the actual data and risks, including any sensitive information that could be revealed or inferred.

11.7 Visibility for SMEs and organisations offering benefits

Ask what information is generated through participation, what reports each participant receives and which customer relationships can be identified. An SME should be able to understand what access it grants through a supply or fulfilment arrangement.

11.8 Responsibility for consequences

The organisation handling the customer relationship may not control every relevant record or decision. Identify who can investigate and correct each stage.

Contracts can allocate commercial responsibilities, but they do not by themselves settle every data-protection role or liability. Compare the arrangement with actual processing.

A fair explanation should make the route to resolution understandable to members as well as suppliers. Unclear responsibility is a problem to address, not an inevitable feature to accept.

11.9 Explain reuse rather than relying on labels

A result may be reused only if the recipient has access to it or observes it through a demonstrable route. Identify that route, the use and its applicable conditions.

If a separate system independently records similar information, explain that collection separately. Similar fields do not prove a common origin.

11.10 Corrections should reach the relevant use

Where an input was wrong or incomplete, identify the dependent records and decisions that need review. A correction in one account does not by itself demonstrate that every recipient updated its copy.

A clear process states who acts, what is checked and how the person receives the outcome. It should preserve the distinction between correcting information and guaranteeing a particular commercial decision.

11.11 Useful access and correction responses

A response should address the person's relevant information and required supplementary information, subject to applicable limits. A list of fields without their meaning can leave an important question unresolved.

Ask what a score, label or code describes, its source and how it is used. Do not assume that an access request compels creation of a new technical report or disclosure of every internal model.

11.12 Design for intelligibility

Usability and transparency should be considered together. People should understand when their information moves into another activity or becomes relevant to another decision.

11.13 Accountability across participants

Identify who can answer, investigate and correct each processing activity. Coordination can help resolve a fragmented question, but it does not replace each organisation's own obligations.

A clear explanation traces the actual interfaces rather than relying on a general statement that no one controls the whole system.

11.14 Section conclusion

The practices described here should be assessed, not presumed acceptable. Some may be justified and well controlled; others may need correction, restriction or cessation depending on the facts and applicable requirements.

The educational objective is to help people distinguish these possibilities. Identify the actual collection, access, connection and use, then examine the responsibilities attached to them.

A useful safeguard should remain explainable. A trusted benefit should support scrutiny rather than use trust as a reason to avoid it.

12. Governance, Visibility and Responsibility

12.1 What complexity changes

Connected systems can create practical difficulties in tracing information, explaining decisions and correcting records. Those difficulties can arise alongside inadequate controls, incomplete responses or other failures; they should not be declared inevitable or excusable in advance.

12.2 What complexity does not change

Applicable duties still attach to the actual processing. A controller cannot treat derived personal information as outside scope merely because the surrounding architecture is complicated.

The issue is not whether a system fits a simple diagram. It is whether responsibilities and explanations are sufficient for the activities performed.

This chapter brings together the technical distinctions and the questions that help reviewers test an account.

12.3 A practical visibility gap

A person may know that a decision occurred without knowing the record or rule behind it. The organisation may need to explain the relevant processing, subject to the applicable rights and limits.

12.4 Compliance must be assessed

The presence of policies, contracts or a familiar technology does not establish compliance. The absence of an immediately understandable explanation does not prove every proposed misuse either.

Compare what was declared with what was collected, connected, retained and used. Identify the applicable purpose and basis at each relevant activity.

A specific mismatch between the explanation and the records is more useful than a blanket assertion about the entire industry.

12.5 SMEs as observers of an unexplained journey

A small business can encounter mismatched identities, unexplained restrictions or fragmented replies while trying to serve its customers. Recording those events carefully can support a review without establishing their cause in advance.

12.6 Why authentication developments matter

EMV 3DS introduced richer contextual exchanges for authentication compared with the first generation. Its deployment history can help frame questions about a period of change.

It does not prove that a particular organisation introduced marketing reuse, continuous behavioural monitoring or cross-merchant matching at that time. Establish deployment dates, versions and surrounding integrations separately.

New product names or later documentation should not be projected backwards as proof of earlier capability. Use dated sources and records relevant to the event.

Source: EMVCo EMV 3-D Secure [1].

12.7 Trust and security questions

A branded benefit can encourage confidence. An attacker may exploit familiarity with a supplier, employer or service community in a deceptive message. This is a risk scenario, not a finding that a particular scheme has been compromised.

12.8 Follow the actual exposure

Ask what information could be obtained, by whom and through which access or failure. A membership label, contact detail and detailed activity history create different risks.

A supplier's technical security, a member's understanding of legitimate messages and the privacy of downstream reporting are related but distinct concerns.

Avoid treating all CUGs as a single security architecture. Evaluate the actual verification, permissions, recipients and response arrangements.

12.9 Keep institutional trust accountable

Employees and members may rely on an organisation's recommendation when joining a benefit scheme. That trust should be supported by a clear account of the external participants and the information they receive.

The organisation offering the benefit should be able to ask about verification, minimisation, reporting access, retention, incident handling and correction routes.

If the answers are incomplete, identify the missing information. If the answers are supported, preserve that evidence too. The point is scrutiny of the actual arrangement, not a predetermined verdict.

12.10 Questions before relying on a reassuring claim

Does 'secure' refer to access controls or to all subsequent uses? Does 'anonymous' describe the recipient's actual ability to identify someone? Does 'not shared' cover selected results and integrations? Does 'closed' describe admission only?

These questions make the boundary between a promotional description and an operational explanation visible.

12.10 What Granular contributes

The paper provides a vocabulary for examining the interfaces between systems: source, purpose, access, match, transformation, recipient and decision. Those terms help turn a broad concern into an answerable question.

12.11 Authentication and surrounding collection

EMV 3DS supports authentication of card-not-present transactions using contextual information. The protocol and a provider's additional fraud tools must be distinguished.

Purpose: authentication for online payments, with risk-based assessment. Authentication and payment authorisation are different stages.

Flow: a frictionless result or a challenge may occur, depending on the assessment and applicable requirements.

Information: transaction, payment and device context varies with channel, version and implementation. This does not establish that every merchant receives every field.

Additional telemetry: provider-specific collection may operate alongside authentication. Continuous session observation or a particular fingerprinting implementation should not be presented as a universal requirement of 3DS2.

Retention and later use: inspect the provider's actual system, permissions and processing purposes. The protocol alone does not establish persistent cross-merchant classification or marketing reuse.

Sources: EMVCo EMV 3-D Secure [1]; Stripe advanced fraud detection [2].

12.12 Integrated and modular systems

An integrated platform and a stack of third-party services can both contain several processing activities. Neither architecture guarantees a single controller, a shared dataset or complete visibility.

In either case, identify the legal entities, purposes, permissions and interfaces. A modular stack may require more hand-off records; a single interface may still conceal multiple recipients.

Signals and interpretations

A session event may describe navigation. An order record may describe purchasing. A payment outcome may reflect authentication, authorisation or other checks. A redemption result may show fulfilment. These are not interchangeable measures of a person's reliability.

If information is combined, ask how the match was made and how the meaning changed. A correlation used in a model should not be presented as a fact about the person without considering its source and uncertainty.

The absence of a bulk dataset exchange does not prove the absence of access to selected results or separate collection. Equally, independent observation does not automatically create cross-system knowledge.

A diagram should name the actual interface or observable outcome that connects its stages.

12.13 Brand context and cross-context analysis

A brand can analyse information about its own relationship with a customer. An intermediary may have access to records across more than one relationship. Whether either has a broader view depends on the actual permissions, identifiers and data supplied.

A CUG does not automatically give an intermediary cross-sector visibility or access to provider-internal risk information. Its membership gate and its reporting architecture are separate features.

Questions for comparison

Scope: which people and transactions are represented? Identifiers: can records be linked across contexts? Access: which organisation can perform that link? Purpose: why is it performed? Accuracy: how are collisions and stale records handled?

Compare evidence rather than assigning universal ratings such as 'high predictive power' or 'low visibility' to an entire model.

A broader dataset may add context, or it may introduce error, irrelevant associations and inappropriate uses. More information is not automatically more reliable or more justified.

12.14 Who gains insight and who carries risk?

An SME may buy stock and retain the customer relationship while another organisation fulfils the benefit. If person-level claims are connected to that stock, the fulfiller may learn about the SME's customer relationships.

That possibility has commercial significance. It should be tested against actual claim mappings, reporting access, contracts and subsequent uses. It is not established by a bulk purchase alone.

Information generated at different stages

Commerce can record orders and customer references. Eligibility can record whether an offer is available. Payment systems can create transaction outcomes. Fulfilment can record completion or failure. A CRM may receive selected records through an integration.

A joined analysis requires a connecting route. Ask whether that route is designed for fulfilment, support, reporting or another use, and whether the relevant people were properly informed.

The critical issue is the relationship between the value created, the explanation given and the responsibilities accepted. A trusted benefit should not be used as a substitute for that explanation.

12.15 The value of context

Purchase frequency, product choice, order value and redemption timing can inform commercial decisions where the information is accessible and usable. They may support stock planning, retention analysis, segmentation or targeting.

The value depends on coverage, accuracy, recency, exclusivity, permissions and the decision being improved. There is no universal price per person or reliable multiplier that can be inferred from the architecture alone.

Fraud telemetry, a visible risk result and ordinary purchase history are different resources. Do not assume that a reporting tool exposes all of them or that a provider monetises them in the same way.

Potential benefit and potential harm

A linked record can help resolve a problem. It can also produce an inaccurate or unwanted classification if the wrong person is matched, context is omitted or a later use exceeds the justified purpose.

The commercial incentive is a reason to ask precise questions. It is not proof that a particular organisation performed the proposed reuse.

Ask: 'Which decisions does this linked information support, who benefits from those decisions, and what information does the person receive about that use?'

12.16 Synthesis: capability, connection and use

A technical explanation must identify the steps between collection and consequence. A system can have a capability without it being enabled. An enabled integration can fail to deliver. A delivered field can remain unused. A used field can be interpreted incorrectly.

EMV 3DS expands contextual authentication; it does not itself establish continuous profiling, a cross-merchant identity graph or permission for marketing reuse.

A shared infrastructure may support several separate purposes and permissions. It is necessary to examine the actual account, integration and processing activity.

When an outcome in one system influences another, identify how it became observable. There may be a report, API response, webhook, reference mapping or separate collection. Do not draw a transfer arrow without establishing the route.

The standard of explanation should be the same for reassuring and concerning accounts. 'We comply' and 'they must be sharing' both need to be tested against the relevant records.

12.17 Boundary lens applied

The boundary is between the activity described to the person and the activity carried out. An explanation of one stage can be accurate yet leave another stage unanswered. That does not determine whether the unanswered activity is lawful or unlawful.

12.18 What follows from this research

The task is to make the assembled journey understandable: identify the participants, trace the fields, distinguish the people involved, establish the purposes and explain consequential decisions.

A provider's legitimate fraud-prevention function does not settle a question about another actor's commercial reuse. Equally, a theoretical reuse route does not show that the actor had access or used it.

Data-protection duties continue to apply to relevant personal information and inferences across these activities. Complexity is not an exemption from accountability.

For an SME or consumer, this framework supports a practical sequence: describe the event; identify the record; ask the bounded question; compare the answer to evidence; and pursue the remaining gap through an appropriate route.

The aim is informed scrutiny. It is neither a promotional account of benefit systems nor a predetermined finding against every participant.

A practical question to take away

Please identify the information used in this decision, the person or account it describes, its source and the purpose for which it was used. Where another system supplied a field or result, please identify the relevant connection and recipient. If the answer concerns only one part of my request, please state what remains outside that answer and why.

Use the version of this question that fits the event. Include a relevant date and reference, but do not send unnecessary identity, medical or payment-card information.

Keep a short table of the question asked, reply received and unresolved point. The aim is to make the remaining gap concrete.

The final pages bring the method together.

Final Conclusion: Making the System Legible

FilmPass's experience led to a broader question: how can a small business or consumer understand a journey assembled from several organisations when the explanations address only individual parts?

Granular offers a method. Follow the source event, the records created, the access available, the matching performed and the decisions that follow. A complete account connects those stages and identifies what remains unknown.

Commercial value can arise from linked information. Harm can arise from inaccurate matches, lost context, excessive collection or unjustified reuse. Whether either occurred in a particular setting depends on evidence of the actual route and use.

A policy can describe an intended purpose without demonstrating that every integration followed it. A product capability can show that something is possible without proving that it happened. A label such as 'fraud prevention' or 'business data' does not remove the need to examine the relevant processing.

The research does not certify the organisations involved as compliant. It also does not replace missing evidence with assumptions. Both disciplines are necessary if the questions are to remain useful and answerable.

For members, employees and SMEs, the essential expectation is intelligibility: who did what with which information, why, and how can an error or unexplained use be challenged?

Granular exists to make those questions easier to ask and harder to leave unanswered.

Reading the research as a whole

Begin with the journey and the people involved. Separate the purchase, payment, authentication, risk, membership and fulfilment records. Then examine the connecting fields and the actual uses.

An explanation is stronger when it states the conditions it depends on and what evidence would disprove it. A missing connection should remain visible as a question.

The paper's critical focus is the difference between a reassuring label and an adequately explained activity. It asks for evidence of both a claimed safeguard and a proposed misuse.

The same discipline protects the value of the research: readers can use it without being asked to accept an unproved conclusion.

Final Reflection: What Becomes Visible When Systems Are Composed

A single benefit can involve admission, purchase, authentication, payment, fulfilment, reporting and support. The person may experience one service while several participants hold different records.

Reading those records together can reveal a supported connection, a missing explanation or a mistaken assumption. The result should be established through the evidence rather than decided in advance.

The same record can acquire another meaning when it is combined with context or used in a different decision. A transaction result is not automatically a judgement about a person. A refund is not automatically evidence of abuse. An eligibility category is not automatically permission for another commercial use.

CUGs make these questions particularly important because affiliation and trust can encourage participation. 'Closed' may describe who receives an offer without describing who receives information about its use.

Where membership, purchases and redemption are linked, ask who benefits from that link and what the person understands. Where no such link is established, retain it as a question rather than a finding.

Accountability should follow the processing across the interfaces that actually exist. Neither a fragmented architecture nor a reassuring label is a complete answer.

The question Granular leaves with the reader

What does this explanation establish, and what does it leave unanswered?

Ask who can access the record, what it means, which person it describes and what happens to it next. Ask whether the answer concerns raw telemetry, an exposed result, a merchant's own records or a separate collection process.

If the route is confirmed, examine its purpose, accuracy, transparency and authority. If the route fails at a stage, record that too. If the answer is incomplete, identify the missing stage precisely.

The value of the research is not that it declares every practice acceptable or every concern proven. It helps people test an account against the information needed to understand it.

An exclusive offer should not close the explanation. A policy should not end a question it has not answered.

Public technical and regulatory references

[1] EMVCo - EMV 3-D Secure. Authentication purpose and contextual information.

[2] Stripe - Advanced fraud detection. Provider-specific collection and distinction from basic 3DS2 device information.

[3] ICO - A guide to subject access: what is the right of access? Personal information and supplementary information.

[4] UK GDPR, Article 5 - principles including purpose limitation, minimisation and accuracy.

[5] ICO - A guide to subject access: can the ICO enforce the right of access? Complaint and enforcement routes.

[6] ICO - Sharing personal information when preventing, detecting and investigating scams and frauds.

Sources describe their published scope. Product features and guidance can change. For a historical event, compare the version and applicable rules at that date. The website's public source directory provides further references for individual worked examples.

FilmPass & Co - Research & Education

Education edition prepared 31 October 2026