



# MITIGATE RISK

Protect your organization from **mail delivery-related fraud** and compliance exposure

GrayHair brings postal intelligence into your enterprise data ecosystem, so risk teams can detect anomalies early and protect high-value communications.

## THE EXECUTIVE PROBLEM

Risk teams are asked to manage fraud and compliance **without reliable visibility into mail delivery behavior**. The consequences of which are:

- Mail theft and interception
- Fraud tied to address manipulation
- Compliance failures due to missed delivery
- Increased exposure to regulatory scrutiny
- Increased fraud-related costs
- Heightened customer concern and tarnished brand



## EXECUTIVE OUTCOMES

With GrayHair's **Enterprise Postal Data Platform**, mail delivery events become visible risk signals.

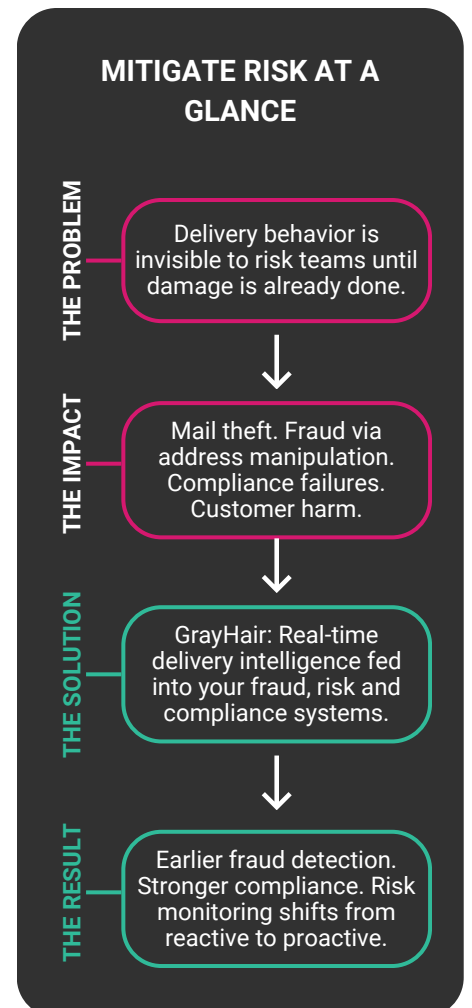
### Typical Enterprise Impact:

- Earlier detection of suspicious mail delivery activity
- Reduced exposure from high-risk destinations
- Prevent sensitive mailings sent to outdated or incorrect addresses
- Stronger compliance posture
- Better coordination between Risk, CX, and Operations
- Increased customer confidence

### What Changes for Risk Leaders?

- Delivery behavior becomes a monitored signal
- Address anomalies surface earlier
- High-value mail is protected
- Compliance failures decline
- Risk teams gain operational efficiency

**YOU CANNOT MANAGE MAIL DELIVERY RISK YOU CANNOT SEE.**



## THE SOLUTION: GRAYHAIR'S ENTERPRISE POSTAL DATA PLATFORM

GrayHair's **Enterprise Postal Data Platform** is a centralized, governed data share that standardizes, enriches, and distributes real-time postal intelligence and insight across enterprise systems. It transforms fragmented mail-tracking, address, and ACS™ data into a secure, integrated asset that powers enterprise-wide analytics, fraud mitigation, customer experience, compliance, and cost optimization.

### When Delivery Is Invisible, Risk Increases

Mail-related risk is rarely obvious at first. It appears as:

- Intercepted cards
- Fraudulent address changes
- Sensitive documents sent to old addresses
- Missed regulatory notices
- Increased customer inquiries and escalations

Without postal intelligence integrated into risk workflows:

- Risk teams react after damage occurs
- Fraud patterns remain hidden
- Compliance issues are discovered too late
- CX teams absorb customer fallout
- Resolution costs mount

**This is not a compliance failure.**  
It is a **visibility failure.**

#### DID YOU KNOW?

Almost 100,000 people in the United States move every day, but only 60% notify the USPS.



## RISK SIGNALS ARE VALUABLE. YOU JUST NEED TO KNOW WHERE TO LOOK.



### Turn Delivery Into a Risk Signal

GrayHair's **Enterprise Postal Data Platform** feeds delivery and address intelligence into fraud systems, risk models, compliance workflows, and analytics platforms. Risk teams gain visibility into:

- Address change patterns
- Delivery failures on sensitive mail
- Return mail tied to regulated communications
- Anomalies that indicate potential fraud or interception

### What Changes in Risk Operations With GrayHair?

- **Earlier Detection:** Suspicious delivery patterns are surfaced before fraud escalates.
- **Fewer Loss Events:** High-risk destinations are suppressed or flagged.
- **Stronger Compliance:** Proof of delivery and visibility into failures support audits and regulatory posture.
- **Better Cross-Team Coordination:** Risk, CX, and Operations work from the same delivery truth.

## DELIVERY INTELLIGENCE CYCLE

CLEANER DATA

BETTER DELIVERY

BETTER CUSTOMER EXPERIENCE

BETTER MARKETING PERFORMANCE

REDUCED RISK AND WASTE

LOWER POSTAL SPEND

REINFORCES DATA QUALITY

## POSTAL INTELLIGENCE DELIVERED!

Every communication generates signals. Those signals generate intelligence. That intelligence improves the next communication and the one after that. This continuous delivery intelligence cycle creates a **self-reinforcing system that improves communications performance across the enterprise.**

### Risk Management Depends on Shared Delivery Visibility

- **Data Quality:** Better address data reduces fraud entry points.
- **Customer Experience:** Fewer delivery failures mean fewer customer harm events.
- **Marketing Effectiveness:** Risk suppression protects campaign integrity and brand trust.
- **Optimized Postal Spend:** High-risk waste is eliminated from mailing programs.

**Risk mitigation improves when delivery becomes visible across the enterprise.**

## INTEGRATIONS ACROSS THE ENTERPRISE

### TURNING SIGNALS INTO ACTION

GrayHair integrates delivery intelligence into the systems where decisions are made.

#### DATA AND ANALYTICS PLATFORMS

- Snowflake, Databricks, BigQuery
- Centralized data lakes and warehouses
- BI tools (Tableau, Power BI, Looker)

**OUTCOME:** Postal data becomes part of the enterprise analytics and AI workflows.

#### CRM, ERP, AND MARKETING PLATFORMS

- Salesforce, HubSpot, Microsoft Dynamics
- SAP, Oracle, NetSuite
- Marketo, Eloqua, Pardot

**OUTCOME:** Better segmentation, timing, targeting, and customer management.

#### CX AND CUSTOMER COMMUNICATIONS

- Contact Centers (Five9, Genesys, NICE, Twilio)
- CCM Platforms (SmartCOMM, Quadient, DataOceans)
- Notification Systems (SendGrid, Twilio, Iterable)

**OUTCOMES:** Real-time communication aligned to actual delivery events.

#### OPERATIONS, RISK, AND COMPLIANCE

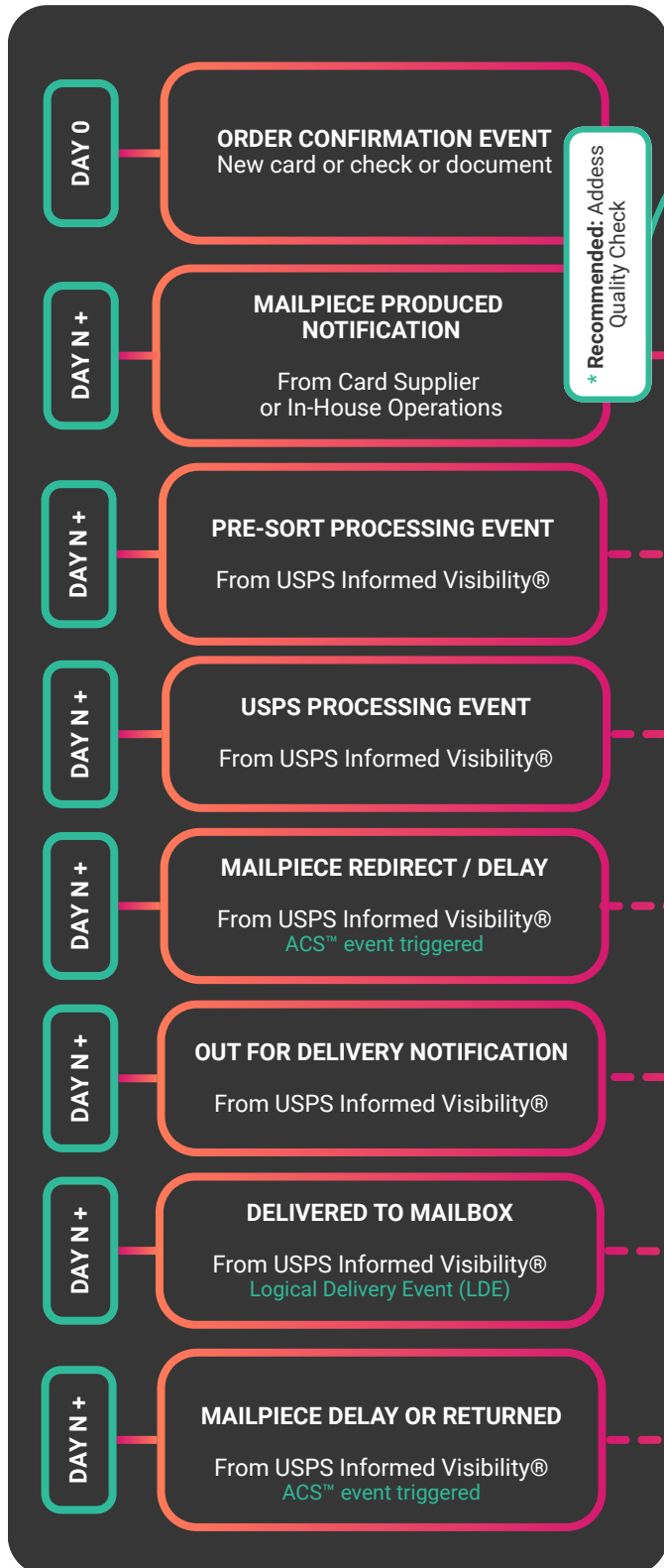
- Fraud detection platforms
- Postal and logistics operations systems
- Compliance and audit systems

**OUTCOMES:** Reduced fraud exposure and improved auditability and operational efficiency.

# POSTAL DATA IN ACTION FOR FRAUD PREVENTION

## SEQUENCE OF MAIL DELIVERY EVENTS

Each postal event is captured by GrayHair across the mail delivery lifecycle, including production through final delivery, redirects, and delays.



## RISK MONITORING

Automated fraud signals and validation checks can be triggered at each event, giving your security team situational awareness.

\* A pre-production address quality check will identify new addresses. This process step provides an early possible fraud alert by pre-empting the redirect process.

### FRAUD SIGNALS

**Validation** that this process step occurred in the predicted time frame

**Validation** that this process step occurred in the predicted time frame

**Validation** that this process step occurred in the predicted time frame

**When the event is received, take action** (possible fraud scenario)

**Validation** that this process step occurred in the predicted time frame

**Validation** that this process step occurred in the predicted time frame

**When the event is received, take action** (possible fraud scenario)



## The Postal Data Center of Excellence (PDCoE)

GrayHair combines technology, process, and expertise to help organizations operationalize postal intelligence.

*Tools + Process + Integrations = Outcomes*

Delivered by GrayHair through the PDCoE – **Postal Data Center of Excellence**

The PDCoE helps enterprises:

- Design delivery intelligence systems
- Implement address quality governance
- Integrate postal data into enterprise platforms
- Continuously improve communications performance

# STOP REACTING. START DETECTING.

Mail-related fraud and compliance failures don't announce themselves. GrayHair makes delivery behavior visible, so risk teams can act before damage occurs.

Transform your risk posture by connecting postal delivery intelligence to your fraud and compliance systems.

## CONTACT US

📞 866-507-9999

✉️ [engage@grayhairsoftware.com](mailto:engage@grayhairsoftware.com)

🌐 [grayhairsoftware.com](http://grayhairsoftware.com)



## ABOUT GRAYHAIR SOFTWARE

GrayHair Software helps the largest financial services, banking, insurance, telco, and healthcare organizations integrate more than 125 billion complex enterprise postal data points (including real-time mail tracking, address quality, and location intelligence) directly into core customer and prospect data platforms. As a result, GrayHair clients achieve dramatic outcomes, including improved marketing campaign performance, enhanced customer communications, reduced undeliverable mail and postal spend, strengthened compliance and fraud measures, and enhanced contact center performance.