A Guide: Fraud Prevention in Produce

October 2025

A collaboration by:

Bill Zentner (Blue Book)
Dante Galeazzi (TIPA)
Ed Treacy (IFPA)
Jamie Bustamante (DRC)
Judy Rudman (USDA/PACA retired)
Kirk Soule (Blue Book)
Mark Benson (Kings River Packing)
Markquell Crooms (The Fresh Connection)
Noel Carreon (TIPA)
Scott Morton (Latitude Group)

1 Introduction

While fraud is not new, over the last several years fraud has evolved and escalated across industries becoming very blatant and aggressive. As examples, the Federal Trade Commission (FTC) reported impersonation fraud is up four-fold in the past year and earlier this year, the Transportation Intermediaries Association (TIA) documented a 68% increase in fraud in just six months. Although this report will focus on impersonation and ghost company fraud due to its prevalence in the industry, fraud comes in a wide variety of different flavors and evolves as the industry gets wise to specific tactics – including double brokering, hacking, cyber theft, ransomware, business email compromise, outright theft of property, etc.

The specialty produce industry is experiencing similar pressures. Blue Book Services is aware of countless impersonation fraud victims, while industry trade groups, along with Blue Book, estimate tens of millions are lost each year to fraudulent buyers. Bad actors target the produce industry's core strengths – speed, relationship-driven deals, and quick decision-making on perishable products.

A recent survey of produce industry participants highlights the issue:

This report provides practical fraud prevention strategies developed by industry practitioners. The objective is straightforward: (1) raise awareness of current fraud tactics, particularly impersonation, shell companies, and product diversion schemes, and (2) deliver actionable solutions that protect our industry's continued success.

2 Problem Statement

The most common impersonation scheme involves a buyer falsely claiming to represent a legitimate third party. The company being impersonated is often, though not always, a recognized name in the produce industry. Similarly, shell (or ghost) company fraud involves the use of fake businesses, or inactive entities with no real operations, created solely to obtain credit and product without any intention of payment.

Bad actors exploit these industry characteristics:

- Produce is perishable, it moves fast, limiting time for thorough vetting
- The industry operates on trust, handshake deals and relationship-driven transactions
- Industry standard credit terms (usually 21-30-days) enable fraudsters to order repeatedly before suspicion arises
- FOB sales may expose companies further by loss of control of delivery
- Sellers are eager for business, so excitement about sales can override caution
- Well-known companies are impersonated, not typically warranting deep checks
- Fraudsters are well-informed, understanding industry standards and markets
- Many companies lack fraud prevention protocols or training
- Jurisdictional gaps exist and cases can fall between authorities (USDA, DRC, local/state police, FBI, RCMP)

Being victimized by fraud isn't a reflection of capacity or capability – it's about bad actors deliberately exploiting industry characteristics that have historically been strengths.

3 The Solution: Best Practices and Tools to Adopt

Buyer impersonation and shell/ghost company fraud may look different on the surface, but both schemes take advantage of weak verification and gaps in oversight. The key to minimizing impact is building strong checks, tightening transaction controls, training staff, and sharing information across the industry. As the saying goes, "an ounce of prevention is worth a pound of cure."

3.1 Strengthen Verification Protocols

Implementing multistep, multisource verification before approving new buyers or representatives is one of the most effective ways to prevent fraud.

Blue Book's review of fraud cases in the produce industry suggests verifying prospective trading partner identities through multiple sources and channels significantly lowers risk.

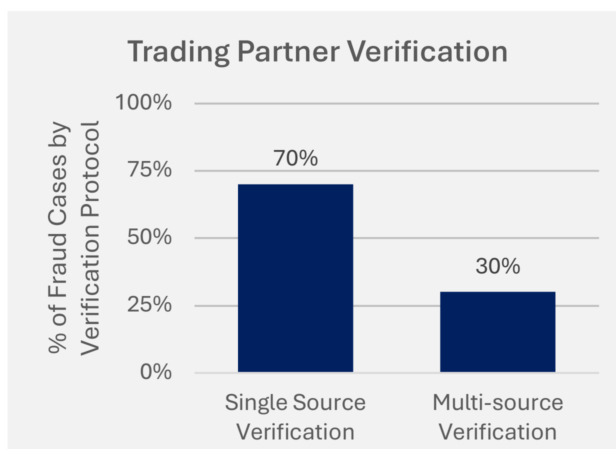

Figure 1: Source Blue Book Analysis

It is highly recommended sellers incorporate these verification channels when evaluating trading partners:

- Trusted third parties: verify buyer identity through multiple trusted sources, such as Blue Book Services, PACA, and DRC.

- Independent verification: validate the published business mailing address, website, email domain (e.g., jdoe@acme-fruit.com → www.acme-fruit.com), phone numbers and/or work history – don't just take the information provided by the subject person or company at face value. This validation can be accomplished through (1) calling another person at the subject company and asking them to confirm the legitimacy of your contact or (2) through Google, LinkedIn and social media searches to validate their identity and tenure.
- Credit check: require a credit application, whether your own application or through Blue Book's Credit Application Check service. The credit application should request information that cannot be obtained publicly, a personal guarantee (optional), a copy of a government ID and the requested credit limit (lookout for unusually high limits). Confirm bank name and that the bank account belongs to the subject company.
- Supporting documentation: request supporting documents like utility bills, lease agreements, and tax IDs for proof of operations.
- Online maps and building images: cross-check listed addresses with maps, online photos, or utility data (shell companies often hide behind PO boxes).

➲ **Red Flag** = look for small differences: misspellings or differences in email addresses, delivery addresses with non-produce names, phone numbers that are different from headquarters (look at the first 3 digits, etc).

➲ **Red Flag** = if a subject company "fails" in one or more of these sources or they are reluctant to provide verifiable references, beware.

Key point: Don't take an inquiry at face value, even if it is from a reliable firm.

3.2 Implement Transactional Safeguards

As a second line of defense after verification, transaction level controls can be equally important in mitigating fraud. These take the shape of Standard Operating Procedures (SOPs).

- Consistent onboarding procedures: an established, clear process for onboarding new partners, especially noting any "pause and verify" rules for any high-risk or high-value transactions. It is recommended that there be a separation of duties between sales and accounting, with accounting owning the only ability to add new customers to the ERP.
- Credit limits: maximum credit limits for any new accounts should be 'locked' in your sales system; accounts can be increased after consistent performance history.
- Approval hierarchies: have a structured process for reviewing credit requests, credit caps, and progressive credit extensions based on performance history.

➲ **Red Flag** = beware of any first-time orders, requesting a break in transactional safeguards (e.g., requesting urgent processing or shipment, delivery to a new address, or unusual payment terms).

Key point: Develop and follow institutional guidelines to mitigate risk.

3.3 Train Teams to Be Alert

Sales, credit, and logistics teams must receive ongoing training to identify fraud tactics.

- Employee training:
    - Warning signs: employees should be trained to look for red flags in emails, phone calls, and orders. This could include bad email domains, inconsistent language in emails, reluctance to provide standard trade references, pressure to bypass normal procedures or less obvious flags like not discussing price or quality (things that other, repeat customers would normally request).
    - SOPs: educate sales account and finance teams on how to vet prospective companies. As noted above, a variety of public and proprietary tools can be leveraged to verify addresses, business and personnel backgrounds, contact information, etc. Understanding the difference in payment types and processes is critical - prepayment, partial payment, check, wire or ACH (e.g., a screenshot of payment confirmation is not sufficient).
- Real-life examples: train with real-life examples and complete fake email and fraud tests to help staff learn. Using real examples breaks down the "it can't happen here" mentality.
- Trust, but verify: encourage a culture of "Trust, but verify."

Key point: Employees are your first line of defense.

3.4 Planning for If Fraud Occurs

Should you suspect you've fallen victim to fraud, an established protocol will allow for a speedy response.

- Internal operations: stop any pending shipments until trading partner verifications have been completed; notify brokers and carriers immediately if a load is still in transit.
- Alert police, insurance: while law enforcement's engagement may be limited by jurisdiction or case load, a police report is usually required to submit an insurance claim.
- Notify industry watchdogs: share relevant details with Blue Book, PACA, and/or DRC to alert other firms of the scheme.

Key point: Response time is critical, so any time lost figuring out how to respond will lower the chances of recovery.

3.5 Working Together Across the Industry

Fraud prevention improves when the entire supply chain communicates. Sharing intelligence about active impersonation or ghost schemes through credit agencies like Blue Book, trade associations, government bodies, and fraud bulletin networks allows faster collective responses.

- When one company reports a scam, others can act before becoming a victim.
- Share fraud alerts, watch lists, and blacklists through trusted channels.
- Encourage transparency, publishing ownership and operational details discourages fraudulent concealment.
- Explore ‘Transparency Scores’ or verification badges to reward openness.

Key point: Sharing fraud experiences and creating awareness strengthens the marketplace.

4 Conclusion

Recent history has shown that even the most seasoned industry veteran can be susceptible to fraud. Bad actors only need you to be too trusting or to make one mistake.

Reducing exposure requires a layered defense – one that blends strong identity checks, secure communication tools, transactional controls, staff vigilance, and shared intelligence across the industry.

By working together and maintaining consistent oversight, businesses can close the gaps fraudsters rely on, building a stronger, more trustworthy marketplace.

A Quick Reference Tool:
Buyer Verification & Fraud Prevention Checklist

1. Verify identity

- Confirm a prospective buyer through trusted sources:
  - ☐ Blue Book (www.bluebookservices.com)
  - ☐ DRC (www.fvdrc.com)
  - ☐ PACA (https://www.ams.usda.gov/rules-regulations/paca)
  - ➲ **Red Flag** = when a company is not listed and/or does not have an active license
- Confirm prospective buyer's identity:
  - ☐ Check phone number and email address matches Blue Book listing
  - ☐ Call the company using the phone number from Blue Book (not from new buyer)
  - ☐ Confirm the identity of the buyer from an independent source at the subject firm
  - ☐ Check the age of the website (www.lookup.icann.org/en) – was it recently created
  - ☐ Confirm the email address domain matches the right company domain (e.g., jdoe@acme-fruit.com → www.acme-fruit.com)
  - ☐ Ensure spelling and addresses match what buyer provides
  - ☐ Verify the business address via Google Earth or Streetview
  - ➲ **Red Flag** = the information does not match the listing or company domain
  - ➲ **Red Flag** = prospect is relucent to provide references or share paperwork
  - ➲ **Red flag** = HQ address is listed as PO box or shared office

2. Establish Credit

- Determine the credit worth of a prospective company:
  - ☐ Require a credit application with references – use your application or Blue Book's Credit Application Request service
  - ☐ Call buyer's Accounting dept.; use number from Blue Book, not from buyer
  - ☐ Recommend using PACA Prompt (10 days) payment terms or a prepayment
  - ☐ Confirm funds are in your bank account before releasing loads
  - ➲ **Red Flag** = do not exceed 30 days as it waives PACA protections
  - ➲ **Red Flag** = first-time orders requesting urgent processing and shipment or delivery (or diversion) to an unapproved address or unusual payment terms

3. Follow-Up

- After the first order has shipped:
  - ☐ Call the Accounting dept.; confirm they have the information necessary to process payment (use the phone number from an independent source like Blue Book)
  - ☐ Report suspicious activity to Blue Book and PACA Investigations

Una Herramienta de Referencia Rápida:
Lista para la Verificación del Comprador y Prevención de Fraud

1. **Verificar Identidad**
   - Confirme a un comprador potencial a través de fuentes confiables:
     ☐ Blue Book (www.bluebookservices.com)
     ☐ DRC (www.fvdrc.com)
     ☐ PACA (https://www.ams.usda.gov/rules-regulations/paca)
     Señal de alerta = cuando una empresa no está en la lista y/o no tiene una licencia activa
   - Confirme la identidad del comprador potencial:
     ☐ Verifique que el número de teléfono y la dirección de correo electrónico coincidan con el listado de Blue Book
     ☐ Llame a la empresa utilizando el número de teléfono que aparece en Blue Book (no el proporcionado por el nuevo comprador)
     ☐ Confirme la identidad del comprador con una fuente independiente dentro de la empresa en cuestión
     ☐ Verifique la antigüedad del sitio web (www.lookup.icann.org/en) – ¿fue creado recientemente?
     ☐ Confirme que el dominio del correo electrónico coincida con el dominio de la empresa (por ejemplo, jdoe@acme-fruit.com → www.acme-fruit.com)
     ☐ Asegúrese de que la ortografía y las direcciones coincidan con lo que el comprador proporciona
     ☐ Verifique la dirección de la empresa mediante Google Earth o Streetview
     Señal de alerta = la información no coincide con la lista o el dominio de la empresa
     Señal de alerta = el comprador es reacio a proporcionar referencias o compartir documentación
     Señal de alerta = la dirección de la sede está registrada como un apartado postal (PO Box) o una oficina compartida

2. **Establecer Crédito**
   - Determine la solvencia crediticia de una empresa potencial:
     ☐ Solicite una aplicación de crédito con referencias – use su propio formulario o el servicio de Solicitud de Aplicación de Crédito de Blue Book
     ☐ Llame al departamento de Contabilidad del comprador; use el número de Blue Book, no el del comprador
     ☐ Se recomienda usar los términos de pago PACA Prompt (10 días) o un pago por adelantado
     ☐ Confirme que los fondos estén en su cuenta bancaria antes de liberar los cargamentos
     Señal de alerta = no exceda los 30 días, ya que se renuncian las protecciones de PACA
     Señal de alerta = pedidos iniciales que solicitan procesamiento urgente y envío o entrega (o desvío) a una dirección no aprobada o con términos de pago inusuales

3. Seguimiento

   - Después de que se haya enviado el primer pedido:
     ☐ Llame al departamento de Contabilidad; confirme que tienen la información necesaria para procesar el pago (use el número de una fuente independiente como Blue Book)
     ☐ Reporte cualquier actividad sospechosa a Blue Book y a las Investigaciones de PACA

A Quick Reference Tool:
Transportation Verification & Fraud Prevention Checklist

Following these best practices, checklist items, and developing a network of trusted and proven providers to handle your loads (including spot loads) is the best way to reduce transportation risk. This paired with a Transportation Service Agreement should provide meaningful coverage for unseen events.

1. Verify Broker or Carrier Identity and Legitimacy

- Confirm a prospective buyer through trusted sources:
  - ☐ Reference the FMCSA database (https://www.fmcsa.dot.gov/) to confirm DOT and MC numbers are active, not just registered. Ensure broker MC authority is valid and insurance coverage is current
  - ☐ Reference other third party services where appropriate (Blue Book Services, Highway, Carrier411, etc.)
  - ➲ **Red Flag** = recently registered companies with limited inspection history
- Verify the Broker's or Carrier's Identity:
  - ☐ Validate that the email domain matches the official company website
  - ☐ Call the company's main office using publicly listed contact info
  - ☐ Request 2–3 shipper references and verify recent business activity
  - ➲ **Red Flag** = mismatched contact details (email domains that are slightly misspelled, phone numbers that have different area codes or prefixes, etc.)
  - ➲ **Red Flag** = recently registered companies with limited inspection history
  - ➲ **Red Flag** = rates significantly below market average
  - ➲ **Red Flag** = lack of concern for cargo handling or delivery specifics

2. Transportation Service Agreement (TSA)

- Standardize your legal agreements with brokers and carriers:
  - ☐ Require a signed TSA before moving freight with a selected broker/carrier. The TSA should include insurance proofs, double-brokering clauses, and terms for liability, payment, tracking, and dispute resolution.
  - ☐ Only bid spot loads with brokers/carriers who have a completed packet and executed TSA
  - ➲ **Red Flag** = redlines to agreements are not necessarily indicative of a bad partner, but they are a way to assess credibility and competency

3. Verify Insurance and Coverage

- Verify appropriate broker and/or carrier insurance:
  - ☐ Request insurance certificates for both broker and carrier

☐ Contact the insurance company directly to ensure: (1) the coverage is valid, (2) your firm is listed as a Certificate Holder, (3) liability and cargo insurance meet or exceed freight value, and (4) your commodity type is covered

➲ **Red Flag** = delays in providing insurance verification can signal issues

4. Validate Drivers and Equipment at Pickup

- Verify driver identity at the guard shack before they get to the dock:
  - ☐ Collect a photocopy of the driver's license
  - ☐ Implement a driver check-in SOP to record driver, vehicle, and trailer details.

5. Monitor for Double Brokering

- Double brokering can present itself in a number of different ways:
  - ☐ Multiple BOLs or mismatched carrier info can signal issues
  - ☐ Use load boards or tracking tools to check if the load was reposted
  - ☐ Work only with brokers who maintain clear load assignment transparency
  - ➲ **Red Flag** = carrier contact info differs from original agreement
  - ➲ **Red Flag** = carrier unfamiliar with load details

6. Assess Load-Specific Risks

- Higher value and/or perishable goods should require special consideration:
  - ☐ Temperature monitoring through the reefer or 3rd party monitoring
  - ☐ Tamper-resistant seals
  - ☐ Restricted delivery zones
  - ☐ Reference NICB data for cargo theft hotspots and adjust routing or insurance

7. Guard Against Payment Scams

- ☐ Use standard payment terms and verify banking details directly with the firm
- ☐ Use third-party monitoring tools to check ratings, complaints, and alerts
- ☐ Join industry fraud bulletin networks

8. Legal Protections

- Include in BOL or Load Tender:

  "The Carrier expressly warrants that it shall transport this shipment under its own operating authority and insurance, and shall not re-broker, assign, transfer, or subcontract any portion of the load without the prior written consent of [Company Name]."

  ➲ **Red Flag** = transportation partner that is unwilling to agree to these terms

Una Herramienta de Referencia Rápida:
Lista de Verificación para la Verificación de Transporte y Prevención de Fraude

1. **Verificar la Identidad y Legitimidad del Corredor o Transportista**
   - Confirme un corredor o transportista potencial a través de fuentes confiables:

     ☐ Consulte la base de datos de la FMCSA (https://www.fmcsa.dot.gov/) para confirmar que los números DOT y MC estén activos, no solo registrados. Asegúrese de que la autoridad MC del corredor sea válida y que la cobertura del seguro esté vigente.

     ☐ Consulte otros servicios de terceros cuando sea apropiado (Blue Book Services, Highway, Carrier411, etc.)

     Señal de alerta = empresas registradas recientemente con historial limitado de inspecciones

   - Verifique la identidad del corredor o transportista:

     ☐ Valide que el dominio del correo electrónico coincida con el sitio web oficial de la empresa

     ☐ Llame a la oficina principal utilizando la información de contacto pública

     ☐ Solicite de 2 a 3 referencias de cargadores y verifique su actividad comercial reciente

     Señal de alerta = detalles de contacto que no coinciden (dominios de correo electrónico mal escritos, números con diferentes códigos de área o prefijos, etc.)

     Señal de alerta = empresas registradas recientemente con poca historia de inspección

     Señal de alerta = tarifas significativamente por debajo del promedio del mercado

     Señal de alerta = falta de interés en el manejo o detalles de la entrega de la carga

2. **Acuerdo de Servicio de Transporte (TSA)**
   - Estandarice sus acuerdos legales con corredores y transportistas:

     ☐ Requiera un TSA firmado antes de mover carga con un corredor/transportista seleccionado. El TSA debe incluir comprobantes de seguro, cláusulas contra la subcontratación doble (double brokering), y términos de responsabilidad, pago, rastreo y resolución de disputas.

     ☐ Solo oferte cargas puntuales (spot loads) con corredores/transportistas que hayan completado su paquete y firmado el TSA.

     Señal de alerta = las modificaciones al acuerdo no siempre indican un mal socio, pero sí sirven para evaluar su credibilidad y competencia.

3. **Verificar Seguros y Cobertura**
   - Verifique que el corredor y/o transportista tengan el seguro adecuado:

     ☐ Solicite certificados de seguro tanto del corredor como del transportista.

     ☐ Contacte directamente a la compañía de seguros para confirmar que: (1) la cobertura sea válida, (2) su empresa esté listada como Titular del Certificado, (3) el seguro de responsabilidad y de carga cubra o supere el valor del flete, y (4) su tipo de mercancía esté cubierto.

Señal de alerta = demoras al proporcionar la verificación del seguro pueden indicar problemas.

4. **Validar Conductores y Equipo en el Punto de Carga**
   - Verifique la identidad del conductor en la caseta de seguridad antes de que llegue al muelle:
     - ☐ Obtenga una fotocopia de la licencia de conducir.
     - ☐ Implemente un procedimiento de registro (SOP) para anotar los datos del conductor, vehículo y remolque.

5. **Monitorear la Subcontratación Doble (Double Brokering)**
   - La subcontratación doble puede presentarse de varias formas:
     - ☐ Múltiples BOLs o información de transportista que no coincide pueden indicar problemas.
     - ☐ Use tableros de carga o herramientas de rastreo para verificar si la carga fue republicada.
     - ☐ Trabaje solo con corredores que mantengan transparencia en la asignación de cargas.

     Señal de alerta = la información de contacto del transportista difiere del acuerdo original.
     Señal de alerta = el transportista desconoce los detalles de la carga.

6. **Evaluar Riesgos Específicos de la Carga**
   - Las cargas de alto valor y/o perecederas requieren consideraciones especiales:
     - ☐ Monitoreo de temperatura mediante el sistema de refrigeración o herramientas externas.
     - ☐ Sellos resistentes a la manipulación.
     - ☐ Zonas de entrega restringidas.
     - ☐ Consulte los datos del NICB sobre puntos críticos de robo de carga y ajuste la ruta o cobertura de seguro según sea necesario.

7. **Protegerse Contra Estafas de Pago**
     - ☐ Use términos de pago estándar y verifique los datos bancarios directamente con la empresa.
     - ☐ Utilice herramientas de monitoreo de terceros para revisar calificaciones, quejas y alertas.
     - ☐ Únase a redes de boletines de fraude de la industria.

8. **Protecciones Legales**
   - Incluya en el BOL o la Orden de Carga (Load Tender):
     - ☐ "El Transportista garantiza expresamente que transportará este envío bajo su propia autoridad operativa y seguro, y que no volverá a subcontratar, asignar, transferir o subcontratar ninguna parte de la carga sin el consentimiento previo por escrito de [Nombre de la Empresa]."

     Señal de alerta = un socio de transporte que se niegue a aceptar estos términos.