Una guía: la prevención del fraude en los productos agrícolas

Octubre de 2025

Una colaboración de:

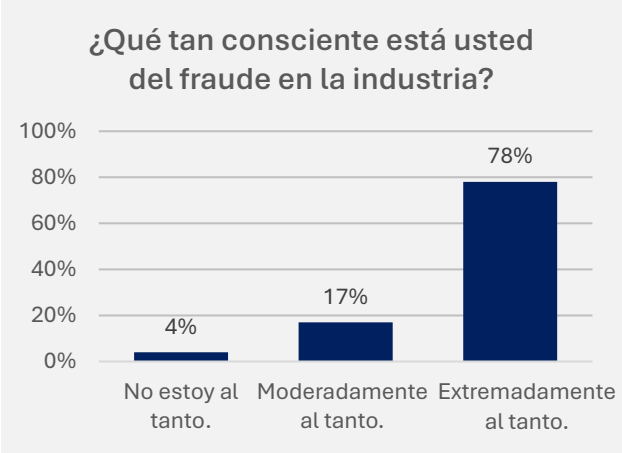
Bill Zentner (Blue Book)
Dante Galeazzi (TIPA)
Ed Treacy (IFPA)
Jamie Bustamante (DRC)
Judy Rudman (jubilada de USDA/PACA)
Kirk Soule (Blue Book)
Mark Benson (Kings River Packing)
Markquell Crooms (The Fresh Connection)
Noel Carreon (TIPA)
Scott Morton (Latitude Group)

1 Introducción

Aunque el fraude no es algo nuevo, en los últimos años evolucionó y se intensificó en todas las industrias, volviéndose muy descarado y agresivo. Por ejemplo, la Comisión Federal de Comercio (FTC) reportó que los fraudes por suplantación de identidad se cuadruplicaron en el último año y, a principios de este año, Transportation Intermediaries Association (TIA) documentó un aumento del 68 % en los fraudes en solo seis meses. Aunque este reporte se centrará en la suplantación de identidad y el fraude de compañías fantasma debido a su prevalencia en la industria, el fraude se presenta de muchas maneras y evoluciona según la industria se vuelve más consciente de tácticas específicas, incluyendo la doble intermediación, la piratería informática, el robo cibernético, el ransomware, el compromiso del correo electrónico de la empresa, el robo directo de propiedad, etc.

La industria de los productos agrícolas especializados está experimentando presiones similares. Blue Book Services conoce innumerables casos de víctimas de fraude por suplantación de identidad, mientras que las asociaciones comerciales del sector, junto con Blue Book, calculan que cada año se pierden decenas de millones debido a compradores fraudulentos. Las personas maliciosas se centran en los puntos fuertes principales de la industria de productos agrícolas: la rapidez, los acuerdos basados en las relaciones y la toma rápida de decisiones sobre productos perecederos.

Una encuesta reciente entre los participantes de la industria de productos agrícolas destaca el problema:



Este reporte proporciona estrategias prácticas para la prevención del fraude desarrolladas por profesionales de la industria. El objetivo es claro: (1) crear conciencia sobre las tácticas de fraude actuales, en particular la suplantación de identidad, las compañías ficticias y los planes de desvío de productos, y (2) entregar soluciones viables que protejan el éxito continuo de nuestra industria.

2 Planteamiento del problema

La estafa más habitual de hacerse pasar por otra persona es cuando un comprador miente y dice que representa a una empresa o persona verdadera. La compañía suplantada suele ser, aunque no siempre, un nombre reconocido en el sector de los productos agrícolas. Del mismo modo, el fraude de compañías ficticias (o fantasma) consiste en el uso de compañías falsas, o entidades inactivas sin operaciones reales, creadas únicamente para obtener crédito y productos sin intención de pagar.

Las personas maliciosas se aprovechan de estas características de la industria:

- Los productos agrícolas son perecederos, se mueven rápidamente, lo que limita el tiempo para una investigación exhaustiva.
- La industria funciona con la confianza, los acuerdos verbales y las transacciones basadas en las relaciones.
- Las condiciones de crédito estándar de la industria (normalmente de 21-30 días) permiten a los estafadores hacer pedidos repetidamente antes de que surjan sospechas.
- Las ventas FOB pueden exponer aún más a las compañías cuando se pierde el control sobre la entrega.
- Los vendedores están ansiosos por hacer negocios, por lo que el entusiasmo por las ventas puede tener más importancia sobre la precaución.
- Se hacen pasar por empresas conocidas, y normalmente no hace falta investigar mucho sobre ellas.
- Los estafadores están bien informados y conocen los estándares y los mercados de la industria.
- Muchas compañías carecen de protocolos o formación para la prevención del fraude.
- Existen lagunas jurisdiccionales y los casos pueden quedar en manos de varias autoridades (USDA, DRC, policía local/estatal, FBI, RCMP).

Ser víctima de un fraude no es un reflejo de su capacidad o aptitud, sino que se trata de personas maliciosas que explotan deliberadamente las características de la industria que históricamente fueron sus puntos fuertes.

3 La solución: mejores prácticas y herramientas para adoptar

La suplantación de identidad del comprador y el fraude de compañías ficticias/fantasma pueden parecer diferentes a simple vista, pero ambos esquemas se aprovechan de la débil verificación y las lagunas en la supervisión. La clave para minimizar el impacto es establecer verificaciones rigurosas, reforzar los controles de las transacciones, formar al personal y compartir información en toda la industria. Como dice el dicho, "es mejor prevenir que lamentar".

3.1 Fortalecer los protocolos de verificación

Implementar una verificación en varios pasos y de múltiples fuentes antes de aprobar nuevos compradores o representantes es una de las maneras más eficaces de prevenir el fraude.

La revisión de Blue Book sobre los casos de fraude en la industria de productos agrícolas sugiere que verificar la identidad de los posibles colaboradores comerciales por medio de múltiples fuentes y canales reduce significativamente el riesgo.

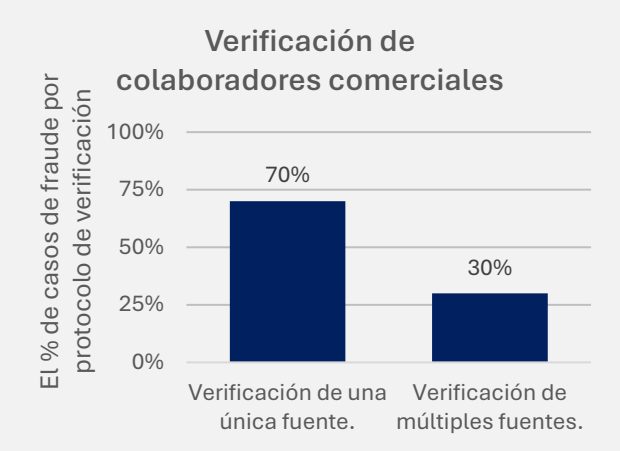


Figura 1: análisis de la fuente de Blue Book

Se recomienda mucho a los vendedores que incorporen estos canales de verificación cuando evalúen a sus colaboradores comerciales:

- Terceros de confianza: verifique la identidad del comprador por medio de múltiples fuentes de confianza, como Blue Book Services, PACA y DRC.
- Una verificación independiente: valide la dirección postal comercial, el sitio web, el dominio de correo electrónico (por ejemplo, jdoe@acme-fruit.com → www.acme-fruit.com), los teléfonos o el historial laboral publicados; no se limite a aceptar sin más la información dada por la persona o compañía sujeto. Esta validación se puede conseguir (1) llamando a otra persona de la compañía sujeto y pidiéndole que confirme la legitimidad de su contacto o (2) mediante búsquedas en Google, LinkedIn y redes sociales para validar su identidad y antigüedad.
- Verificación de crédito: se exige una solicitud de crédito, ya sea su propia solicitud o por medio del servicio de verificación de solicitudes de crédito de Blue Book. La solicitud de crédito debe pedir información que no se pueda obtener públicamente, una garantía personal (opcional), una copia de un documento de identificación oficial y el límite de crédito solicitado (preste atención a los límites inusualmente altos). Confirme el nombre del banco y que la cuenta bancaria pertenezca a la compañía sujeto.
- Documentación justificativa: solicite documentos que respalden como facturas de servicios públicos, contratos de alquiler y números de identificación fiscal como prueba de las operaciones.
- Mapas en línea e imágenes de edificios: compare las direcciones indicadas con mapas, fotos en línea o datos de servicios públicos (las compañías ficticias suelen ocultarse tras apartados de correos).

- **Bandera roja** = busquen pequeñas diferencias: errores ortográficos o diferencias en las direcciones de correo electrónico, direcciones de entrega con nombres que no son de productos, teléfonos diferentes a los de la sede central (fíjense en los 3 primeros dígitos, etc.).
- **Bandera roja** = si una compañía sujeto de estudio "falla" en una o más de estas fuentes o parece no estar dispuesta a dar referencias verificables, hay que tener cuidado.

Punto clave: no se fíe de las consultas a primera vista, aunque procedan de una compañía fiable.

3.2 Implemente medidas de seguridad transaccionales

Como segunda línea de defensa después de la verificación, los controles a nivel de transacción pueden ser igualmente importantes para atenuar el fraude. Estos adoptan la forma de procedimientos operativos estándar (SOP).

- Procedimientos de incorporación coherentes: un proceso establecido y claro para incorporar nuevos colaboradores, prestando especial atención a las normas de "pausa y verificación" para cualquier transacción de alto riesgo o alto valor. Se recomienda que haya una separación de funciones entre ventas y contabilidad, y que únicamente contabilidad tenga la capacidad de agregar nuevos clientes al ERP.
- Límites de crédito: los límites máximos de crédito para cualquier cuenta nueva deben "bloquearse" en su sistema de ventas; las cuentas pueden aumentarse después de un historial de rendimiento constante.
- Jerarquías de aprobación: tener un proceso estructurado para revisar las solicitudes de crédito, los límites de crédito y las ampliaciones progresivas de crédito basadas en el historial de rendimiento.

- **Bandera roja** = tenga cuidado con los pedidos nuevos que soliciten una ruptura de las medidas de seguridad transaccionales (por ejemplo, que soliciten un procesamiento o envío urgente, una entrega a una nueva dirección o condiciones de pago inusuales).

Punto clave: Desarrolle y siga las directrices institucionales para atenuar el riesgo.

3.3 Forme a sus equipos para que estén alerta

Los equipos de ventas, crédito y logística deben recibir formación continua para identificar las tácticas de fraude.

- Formación de los empleados:
  - Señales de alerta: se debe formar a los empleados para que detecten señales de alerta en correos electrónicos, llamadas de teléfono y pedidos. Esto podría incluir dominios de correo electrónico sospechosos, lenguaje poco coherente en los correos electrónicos, poca disponibilidad a dar referencias comerciales estándar,

presión para eludir los procedimientos normales o señales menos obvias, como no hablar del precio o la calidad (cosas que otros clientes habituales normalmente solicitarían).
    - SOP: formar a los equipos de ventas y finanzas sobre cómo evaluar a las compañías potenciales. Como se mencionó arriba, se pueden usar diversas herramientas públicas y privadas para verificar direcciones, historias comerciales y personales, información de contacto, etc. Es fundamental comprender la diferencia entre los tipos y procesos de pago: prepago, pago parcial, cheque, transferencia bancaria o ACH (por ejemplo, una captura de pantalla de la confirmación del pago no es suficiente).
- Ejemplos de la vida real: entrene con ejemplos de la vida real y complete pruebas sobre correos electrónicos falsos y fraudes para ayudar al personal a aprender. El uso de ejemplos reales rompe con la mentalidad de "aquí eso no puede pasar".
- Confíe, pero verifique: fomente una cultura de "confíe, pero verifique".

Punto clave: los empleados son su primera línea de defensa.

3.4 Planificación en caso de fraude

Si sospecha que es víctima de un fraude, existe un protocolo establecido que le permitirá obtener una respuesta rápida.

- Operaciones internas: detengan cualquier envío pendiente hasta que se completen las verificaciones de los colaboradores comerciales; avisen inmediatamente a los agentes y transportistas si una carga aún se encuentra en tránsito.
- Avisar a la policía y al seguro: aunque la intervención de las fuerzas del orden público puede verse limitada por la jurisdicción o el volumen de casos, normalmente se necesita un reporte policial para presentar un reclamo al seguro.
- Avise a los organismos reguladores de la industria: comparta la información pertinente con Blue Book, PACA o DRC para alertar a otras compañías sobre la estafa.

Punto clave: el tiempo de respuesta es fundamental, por lo que cualquier tiempo perdido en decidir cómo responder reducirá las posibilidades de recuperación.

3.5 Trabajando juntos en toda la industria

La prevención del fraude mejora cuando se comunica toda la cadena de suministro. Compartir información sobre suplantaciones de identidad activas o estafas fantasmas por medio de agencias de crédito como Blue Book, asociaciones comerciales, organismos gubernamentales y redes de boletines sobre fraudes permite dar respuestas colectivas más rápidas.

- Cuando una compañía reporta una estafa, otras pueden actuar antes de convertirse en víctimas.
- Comparta alertas de fraude, listas de vigilancia y listas negras mediante los canales de confianza.

- Fomentar la transparencia, publicar los datos sobre la propiedad y el funcionamiento desalienta el ocultamiento fraudulento.
- Explore las "puntuaciones de transparencia" o insignias de verificación para recompensar la transparencia.

Punto clave: compartir experiencias sobre fraudes y crear conciencia fortalece el mercado.

4 Conclusión

La historia reciente muestra que incluso los veteranos más experimentados de la industria pueden ser susceptibles al fraude. Las personas maliciosas solo necesitan que sea confiado o que cometa un solo error.

Para reducir la exposición se necesita una defensa por capas, que combine verificaciones de identidad rigurosas, herramientas de comunicación seguras, controles transaccionales, vigilancia del personal e intercambio de información entre toda la industria.

Cuando se trabaja juntos y se mantiene una supervisión constante, las empresas pueden cerrar las brechas de las que se aprovechan los estafadores, creando así un mercado más sólido y confiable.

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

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.