2026 International Client Seminar

March 5-7, 2026

Small World, Big Schemes

Navigating the Global Landscape of Payment Fraud Litigation

Rachel Hytken
Moderator
QUILLING SELANDER LOWNDS WINSLETT & MOSER, P.C.
Dallas, Texas
rhytken@qslwm.com

Daniel Peterson
COSGRAVE VERGEER KESTER LLP
Portland, Oregon
dpeterson@cosgravelaw.com

Brendan Taylor
MILLS OAKLEY
Perth, Australia
btaylor@millsoakley.com.au

Overview

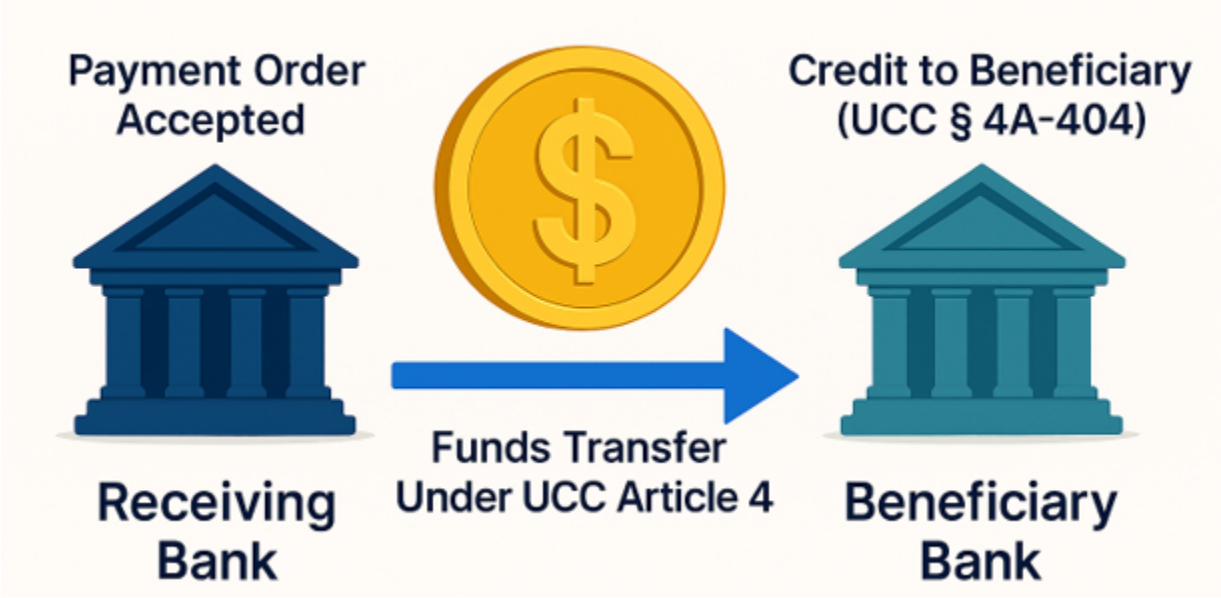
The days of the "Nigerian prince" email are behind us. Fraudsters have become increasingly sophisticated in engineering payment fraud schemes. According to Visa Acceptance Solutions' 2025 Global eCommerce Payments & Fraud Report, 80% of merchants saw an increase in the use of real-time payment fraud over the past year and the same number of merchants struggle with using data and technology to manage fraud. This fraud succeeds in large part due to human error, and when it strikes on a magnitude--in the case of Essilor Thailand--of $272 million dollars, it can have devastating consequences to the business.

This article discusses the framework for financial fraud under the Uniform Commercial Code and compares that approach to the landmark scam prevention framework codified in Australia.

Customer Liability and Defenses

Loss Allocation Framework Under UCC Article 4A

In the context of wire fraud liability, the fraudster is often a difficult target. UCC Article 4a allocates liability among the fraudsters' victims through an interlocking framework of sections 4A-202, 4A-203, and 4A-204 that creates a risk allocation scheme between customers, receiving banks (the financial institution receiving the payment order), and beneficiary banks (the financial institution to which the funds transfer for the benefit of the recipient account holder).



The default rule requires banks to bear losses from unauthorized wire transfers, but this liability shifts to customers when banks implement commercially reasonable security procedures and comply with them in good faith. UCC § 4A-202. Receiving banks have limited liability beyond express contractual obligations and are not agents of transaction parties. Beneficiary banks primarily face liability for failure to pay beneficiaries after acceptance or for inadequate notice. Customers can defend against liability by proving fraud was not caused by entrusted persons or those with access to customer-controlled systems. However, they must provide timely notice within 90 days to preserve interest claims on refunds.

Authorization and Effectiveness Standards

Customer liability for wire fraud losses depends primarily on whether the payment order was "authorized" under section 4A-202(a) or "effective" under section 4A-202(b). A payment order is authorized if "that person authorized

the order or is otherwise bound by it under the law of agency." UCC § 4A-202. Courts have found customers liable even when they were defrauded into authorizing transfers, as in *Niram, Inc. v. Sterling Nat'l Bank*, where the court held that employees had actual authority to initiate transfers despite following fraudulent instructions received via compromised email. *Niram, Inc. v. Sterling Nat'l Bank*, 697 F.Supp.3d 15 (2023).

The effectiveness standard under section 4A-202(b) applies when "a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure" that is both commercially reasonable and properly followed by the bank in good faith. UCC § 4A-202. This provision creates a safe harbor for banks that implement adequate security measures.

Commercial Reasonableness of Security Procedures

The determination of whether security procedures are commercially reasonable is "a question of law" that courts must decide by "considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated." UCC § 4A-202.

Courts have reached different conclusions on commercial reasonableness based on specific factual circumstances. In *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, the Eighth Circuit found that security procedures including "password protection, daily transfer limits, device authentication" were commercially reasonable, particularly where the customer declined additional security measures requiring dual approval. *Choice Escrow and Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611 (2014) Conversely, in *Patco Constr. Co. v. People's United Bank*, the First Circuit determined that basic Internet banking security procedures were not commercially reasonable for the particular customer's circumstances. *Patco Constr. Co., Inc. v. People's Utd. Bank*, 684 F.3d 197 (1st Cir. 2012).

As the First Circuit explained in, there are two ways by which a security procedure may be shown to be commercially reasonable. First is by reference to:

> [T]he wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer and security procedures in general use by customers and receiving banks similarly situated.

Id. § 4–1202(3). The Article is explicit that "[t]he standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank...." *Id.* § 4–1203 cmt. 4. The UCC explains that "[t]he burden of making available commercially reasonable security procedures is imposed on receiving banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud." *Id.* cmt. 3.

Secondly, the Article creates a presumption of reasonableness under certain circumstances, not applicable here. A security procedure is deemed to be commercially reasonable if:

(a) The security procedure was chosen by the customer after the bank offered and the customer refused, a security procedure that was commercially reasonable for that customer; and

(b) The customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.

Id. § 4–1202(3). Of course, if the security procedure offered by the bank was not commercially reasonable, then the provision does not apply. *Id.* § 4–1203 cmt. 4.

Customer Defenses Under Section 4A-203

Section 4A-203(2) provides customers with a critical defense against liability for unauthorized, but effective payment orders. Customers can escape liability if they prove "the order was not caused, directly or indirectly, by a person (i) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or (ii) who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure." UCC § 4A-203. If the customer can prove that the person committing the fraud did not obtain the confidential information needed to perpetrate the fraud from an agent or former agent of the customer or from a source controlled by the customer, the loss is shifted to the bank. “Prove” is defined in Section 4A-105(a)(7). Internal investigation records of the bank or by bank examiners as well may develop evidence of who is at fault and the cause of the loss. The customer may gain access through discovery to evidence developed in these investigations, and that evidence can be used by the customer in meeting its burden of proof.

Notice Requirements and Timing

Section 4A-204(a) establishes important notice requirements that affect customer rights to recover interest on unauthorized transfers. While banks must refund unauthorized payments, "the customer is not entitled to interest from the bank on the amount to be refunded if the customer fails to exercise ordinary care to determine that the order was not authorized by the customer and to notify the bank of the relevant facts within a reasonable time not exceeding 90 days after the date the customer received notification from the bank that the order was accepted or that the customer's account was debited." UCC § 4A-204. Importantly, this timing requirement affects only interest entitlement, not the underlying refund obligation.

Receiving Bank Liability

Receiving banks operate under a limited liability framework established by section 4A-212, which states that banks have no general "duty to accept a payment order or, before acceptance, to take any action, or refrain from taking action, with respect to the order except as provided in this Article or by express agreement." UCC § 4A-212. The statute explicitly provides that "a receiving bank is not the agent of the sender or beneficiary of the payment order it accepts, or of any other party to the funds transfer, and the bank owes no duty to any party to the funds transfer except as provided in this Article or by express agreement." UCC § 4A-212.

Receiving banks can incur liability either through breach of express agreements to accept payment orders or upon acceptance of payment orders as defined in section 4A-209, and in both cases "liability is limited to that provided in this Article." UCC § 4A-212. This creates a narrow scope for receiving bank liability that primarily encompasses situations where banks fail to meet express contractual obligations or violate specific Article 4A requirements.

Beneficiary Bank Obligations and Liability

Beneficiary banks face distinct obligations under sections 4A-209(b) and 4A-404 that create limited but specific liability exposure. Section 4A-209(b) defines when beneficiary banks accept payment orders, which occurs "at the earliest" of several triggering events including when the bank "pays the beneficiary" or "receives payment of the entire amount of the sender's order." UCC § 4A-209.

Once acceptance occurs, section 4A-404(a) creates a mandatory payment obligation: "if a beneficiary's bank

accepts a payment order, the bank is obliged to pay the amount of the order to the beneficiary of the order." UCC § 4A-404. Failure to pay after acceptance can result in liability for consequential damages if "the bank refuses to pay after demand by the beneficiary and receipt of notice of particular circumstances that will give rise to consequential damages." UCC § 4A-404.

Beneficiary banks also face liability for notice failures under section 4A-404(b), which requires notification to beneficiaries "before midnight of the next funds-transfer business day following the payment date" for account-based transfers. UCC § 4A-404 Banks that fail to provide required notice must "pay interest to the beneficiary on the amount of the payment order from the day notice should have been given until the day the beneficiary learned of receipt of the payment order by the bank." UCC § 4A-404.

Preemption of State Law Claims

UCC Article 4A provides a comprehensive but limited preemption of state law claims in wire fraud litigation. The Second Circuit has applied a fact-specific analysis examining whether Article 4A's provisions "protect against the type of underlying injury or misconduct alleged in a claim." *Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc*., 597 F.3d 84 (2010). Article 4A preempts common law claims that would create rights, duties, and liabilities inconsistent with its provisions, but does not provide blanket field preemption. State law claims based on conduct occurring outside the wire transfer process—such as actions before or after the transfer mechanics, or additional fraudulent conduct beyond the transfer itself—are generally not preempted. The preemption analysis focuses on whether the disputed conduct falls squarely within Article 4A's coverage rather than simply whether a wire transfer was involved in the underlying facts.

Conflict Preemption – the mechanical and temporal tests

Because UCC 4a is limited to conflict preemption, not field preemption, a litigant may pursue state law claims that survive the mechanical test or temporal test. The Second Circuit in *Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc.* applied a critical inquiry test that asks "whether its provisions protect against the type of underlying injury or misconduct alleged in a claim." This test requires courts to examine the specific nature of the alleged misconduct rather than simply whether a wire transfer was involved in the factual scenario. The Second Circuit in *Ma* explained that "Practically speaking, Article 4A controls how electronic funds transfers are conducted and specifies certain rights and duties related to the execution of such transactions. Claims that, for example, are not about the mechanics of how a funds transfer was conducted may fall outside of this regime." *Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 597 F.3d 84 (2010). This "mechanics" test has become a key framework for determining preemption boundaries.

The Seventh Circuit further clarified that "A common law claim is not 'per se inconsistent with [Article 4A's] regime' merely because the alleged facts include a wire transfer." *Approved Mortgage Corp. v. Truist Bank*, 106 F.4th 582 (2024). Courts must determine whether Article 4A's provisions specifically protect against the type of misconduct alleged, not whether wire transfers are tangentially related to the claims.

Opening and Management of Accounts Exception

Courts have recognized an important exception for claims related to bank account opening and management that facilitate wire fraud schemes, even when those accounts ultimately receive fraudulent wire transfers. In *Tex. Star Nut & Food Co. v. Truist Bank*, 632 F.Supp.3d 664 (D. Maryland 2022), the District of Maryland held that "common law allegations, to the extent they stem from the opening and management of the hacker's bank account, are not preempted by Article 4A of the UCC."

This exception recognizes that banks' duties regarding customer onboarding, due diligence, and account monitoring

exist independently of their obligations under Article 4A regarding wire transfer processing. Such claims focus on the bank's role in facilitating fraud through negligent account practices rather than on the wire transfer mechanics themselves.

Courts have developed a temporal analysis for determining preemption boundaries, distinguishing between conduct occurring before, during, and after the wire transfer process. The Northern District of New York established in *Pedersen v. MidFirst Bank*, 527 F.Supp.3d 188 (2021), that claims based on MidFirst's actions before and after the processing of the wire transfer are not preempted because the U.C.C. wire transfer provisions do not address a bank's duties outside of the mechanics of administering a wire transfer.

However, claims directly related to the processing and execution of wire transfers are consistently preempted. The Eastern District of New York held in *McCarthy v. JP Morgan Chase Bank*, 772 F.Supp.3d 298 (2025), that a negligence claim alleging a bank's failure to warn a customer about likely wire fraud was preempted because "a bank's security procedures pertaining to the acceptance of a payment order is one of the 'mechanics of wire transfers.'"

The distinction becomes clearer when examining specific examples. In *Henderson v. Wells Fargo Bank*, 779 F.Supp.3d 910 (2025), the Southern District of Texas held that "Article 4A does not preempt Plaintiff's negligence claims relating to failures before the transfer" such as duties to prevent unauthorized access, because these "do not relate to the wire transfer itself and are not covered by Article 4A." Similarly, negligence claims "to the extent they arise out of Defendant's failure to train its employees" were not preempted as they "did not fall squarely within Article 4A's ambit."

Knowledge-Based Fraud Claims: The Regions Bank Exception

An important exception to preemption exists for claims against banks that knowingly process fraudulent transfers. The Eleventh Circuit in *Regions Bank v. Provident Bank, Inc.*, 345 F.3d 1267 (2003), established that "Article 4A is silent with regard to claims based on the theory that the beneficiary bank accepted funds when it knew or should have known that the funds were fraudulently obtained." The court held that "a provision of state law that requires a receiving or beneficiary bank to disgorge funds that it knew or should have known were obtained illegally when it accepted a wire transfer is not inconsistent with the goals or provisions of Article 4A."

This principle has been applied broadly to protect claims against banks with actual or constructive knowledge of fraudulent transfers. The Southern District of Indiana in *BMO Harris Bank N.A. v. Salin Bank & Trust Co.*, 750 F.Supp.3d 1041 (2024), held that Article 4A "does not provide the exclusive governing body of law for common law claims" when they are "based on a theory that a beneficiary bank accepted funds with the actual or constructive knowledge that the transfer was done in error."

However, courts distinguish between claims requiring actual knowledge of fraud and general negligence claims that would impose broader duties. The Southern District of Texas noted in *Peatwatuck Enterprises v. Truist Bank*, 773 F.Supp.3d 366 (2025), that negligence claims are preempted by Article 4A due to Article 4A's comprehensive scheme governing funds transfers.

Australia's Scam Prevention Framework

The Scams Prevention Framework Act 2025 (Cth) was passed in early 2025 to introduce the Scams Prevention Framework (SPF) through extensive amendments to Australian consumer protection legislation, namely the *Competition and Consumer Act 2010* (Cth).

The SPF imposes obligations on both local and overseas entities in banking, telecommunications, and digital platforms to take "reasonable steps" to support consumers in avoiding scams. Its objective is to protect Australian

small business, consumers in Australia, and Australian residents abroad using services connected to Australia. CCA s 58AA. The law's overarching principles are: (1) Governance, (2) Prevent, (3) Detect, (4) Report, (5) Disrupt and (6) Respond. CCA, Part IVF, sub-divs 2-6.

The initial stages of the SPF are due to commence operation on 1 July 2026 and be fully implemented by the end of 2027. In the interim, the Australian Government has recently undertaken public consultation to establish sector specific codes under section 58AB of the CCA.

These codes would apply to businesses in sectors designated under the SPF (designated sectors) including the banking, telecommunications, and digital platforms (social media, search engine and instant messaging services) sectors. The codes cannot create offences or amend the legislative framework but will outline the minimum steps that these businesses must take to meet SPF obligations and other prescribed matters.

A review of the SPF's operation must be conducted three years after the first SPF code is made, with a report tabled in Parliament.

Initial public consultation on the codes occurred in late 2025 and closed on 6 January 2026 with additional public consultation intended throughout 2026.

Overarching Principles of the SPF

Governance refers to the requirement for each regulated entity to establish comprehensive written risk-management policies, to develop metrics and targets to evaluate the efficacy of the polices, to continuously assess and address the risks of scams; to make information available to consumers on how to report scams, to ensure annual review and approval of the policies and procedures, and to maintain records of activities taken to comply with the SPF for six years. CCA s 58BC.

Prevention refers to the requirement that each regulated entity for a regulated sector must take reasonable steps to prevent scams. The SPF code for the sector may include sector-specific provisions for this principle. A regulated entity contravenes this subsection if the entity fails to take reasonable steps to prevent another person from committing a scam relating to, connected with, or using a regulated service of the entity. CCA s 58BI.

Detection refers to the duty of each regulated entity to take reasonable steps to detect scams. This includes: (a) investigating, in a timely way, activities that are the subjects of its actionable scam intelligence; and (b) identifying, in a timely way, its consumers that have or may have been impacted by such activities. The SPF code for the sector may include sector-specific provisions for this principle. CCA s 58BL.

Report means that each regulated entity must give the SPF general regulator reports of any actionable intelligence the entity has about activities relating to, connected with, or using the entity's regulated services. A regulated entity must give an SPF regulator a report about a scam if the SPF regulator requests. The SPF general regulator may disclose information about scams to certain other entities. CCA s 58BQ.

Disrupt means each regulated entity for a regulated sector must take reasonable steps to: (a) disrupt an activity that is the subject of actionable scam intelligence; and (b) prevent losses from such an activity. The entity will also need to report to the SPF general regulator the outcomes of the entity's investigation about whether such an activity is a scam. The report may also need to describe any disruptive actions the entity has taken in relation to the activity. The entity is not liable for damages etc. in taking certain actions to disrupt such an activity. CCA s 58BW.

Respond means that each regulated entity must have an accessible mechanism for its consumers to report activities

that are or may be scams. The entity must have an accessible and transparent internal dispute resolution mechanism for its consumers to complain about: (a) activities that are or may be scams; or (b) the entity's conduct relating to such activities. The entity must publish information about these mechanisms. When undertaking such internal dispute resolution about a complaint, the entity must give a statement, relevant to the complaint, about whether it has complied with its obligations. When undertaking such internal dispute resolution, the entity must have regard to: (a) any processes prescribed by the SPF rules; and (b) any guidelines prescribed by the SPF rules for apportioning any liability. The entity must become a member of an authorized external dispute resolution scheme for dealing with complaints about scams if the entity provides services regulated by the Scams Prevention Framework. CCA s 58BZB.

Injunctions and Actions for Damages

The legislation empowers the Australian Competition and Consumer Commission (ACCC) to regulate compliance; those who breach their obligations can include penalties of up to AUD50 million for non compliance. It also creates a private right of action. Victims of conduct contravening an SPF principle or code can recover damages, with claims made within six years of the cause of action. Proportionate liability applies to concurrent wrongdoers, limiting their liability to their share of responsibility. Additionally, the SPF contemplates possible injunctions to prevent or require actions if a person is involved in conduct that contravenes a civil penalty provision of an SPF principle or code.

The framework establishes roles for SPF regulators, information sharing between regulators, and enforcement mechanisms including civil penalties, infringement notices, and injunctions. The Commission is the general regulator, with other entities potentially regulating specific sectors. Civil penalties apply for non-compliance with the framework's principles and codes, with maximum penalties specified for different contraventions. Remedies for contraventions include infringement notices, enforceable undertakings, injunctions, and actions for damages.

Public Warning Notices and Remedial Directions

SPF regulators can issue public warnings if they suspect conduct contravenes SPF principles or codes and if it is in the public interest. Notices must be published on the regulator's website. Regulators can direct entities to comply with SPF principles or codes if non-compliance is suspected, with non-compliance being a civil penalty.

Adverse Publicity, Non-Punitive Orders, and Redress

Courts can order adverse publicity for entities penalized under SPF provisions. Non-punitive orders, such as community service or probation, can be made for contraventions. Courts can make orders to redress loss or damage caused by contraventions, including contract voiding or refunds, with applications made within six years of the cause of action.

Treatment of Partnerships, Associations, and Trusts

SPF provisions apply to partnerships, unincorporated associations, and trusts as if they were individuals, with obligations imposed on partners, committee members, or trustees.

Compensation for Property Acquisition and Rules

If SPF provisions result in property acquisition without just terms, compensation must be paid.

Choice of Law Issues

Domestic US Wires

UCC Article 4A Section 507 provides specific choice of law rules that determine which state's version applies to

domestic wire fraud cases. The statute establishes a hierarchical framework with three primary mechanisms for determining governing law.

Default Location-Based Rules: When parties haven't made specific agreements, UCC 4A-507 applies location-based rules where rights and obligations between the sender and receiving bank are governed by the law of the jurisdiction where the receiving bank is located, rights between the beneficiary's bank and beneficiary are governed by the law where the beneficiary's bank is located, and the timing of payment from originator to beneficiary is governed by the law where the beneficiary's bank is located. This creates a clear default system based on bank locations rather than traditional conflict of laws analysis.

Party Choice of Law Agreements: The statute grants parties broad freedom to select governing law through agreement, providing that if parties have made an agreement selecting the law of a particular jurisdiction, that law governs their rights and obligations, regardless of whether the payment order or funds transfer bears a reasonable relation to that jurisdiction. This provision gives maximum freedom of choice and creates strong incentives to choose jurisdictions where Article 4A is in effect because it provides greater certainty regarding parties' rights. When there are conflicts between party agreements and system rules, the party agreements prevail.

Funds Transfer System Rules: A funds-transfer system may select the law of a particular jurisdiction to govern rights and obligations between participating banks or the rights and obligations of parties to a funds transfer carried out through the system . These system choices bind participating banks and other parties when they have notice that the system might be used and of the system's choice of law. This provision may be the most important for creating uniformity, as funds transfer systems will likely adopt governing law to increase transaction certainty, potentially choosing Article 4A states to provide consistent, unitary law governing all system transfers.

The statute addresses the interstate character of funds transfers by noting that without uniform governing law, it becomes very difficult to predict results when problems arise because there is no clear consensus among jurisdictions concerning the juridical nature of these transactions. This framework effectively displaces traditional conflict of laws analysis for wire transfers covered by Article 4A, providing certainty about which state's UCC provisions apply even when those provisions are not uniform between states.

If a funds transfer is made by use of more than one funds transfer system and there is inconsistency between choice-of-law rules of the systems, the matter in issue is governed by the law of the selected jurisdiction that has the most significant relationship to the matter in issue.

Forum Selection and Choice of Law Clauses for International Wires

International wire fraud cases frequently involve contractual forum selection and choice of law clauses that courts must evaluate for enforceability. The Supreme Court in *Scherk v. Alberto-Culver Co.*, 417 U.S. 506 (1974), established that arbitration clauses (which the Court characterized as "a specialized kind of forum-selection clause") in international contracts should be enforced unless "the inclusion of that clause in the contract was the product of fraud or coercion." This standard requires fraud specific to the clause itself, not merely general allegations of fraud in the underlying transaction.

Lower courts have consistently applied this principle to forum selection clauses, holding that "to render a forum selection clause unenforceable, the party seeking to avoid the clause must show that the clause itself was procured by fraud" *Edge Telecom, Inc. v. Sterling Bank*, 143 P.3d 1155 (2006). The Colorado Court of Appeals explained that "so long as a forum selection clause is itself not the result of fraud, the parties can fairly expect to litigate any issues, including the plaintiff's general allegations of fraud, in the designated forum."

This framework provides significant predictability for international parties, as courts will not invalidate forum selection clauses based solely on fraud allegations about the underlying business transaction. The clause-specific fraud requirement creates a high bar for avoiding contractual forum provisions in international wire fraud cases.

Extraterritoriality and Domestic Application Tests for International Wires

International wire fraud cases require courts to determine whether federal wire fraud statutes apply extraterritorially or constitute permissible domestic applications of federal law. Circuit courts have developed varying approaches to this analysis. The Fourth Circuit in *United States v. Elbaz*, 52 F.4th 593 (2022), held that "the focus of the wire-fraud statute, for purposes of identifying a permissible domestic application for the statute, is the use of a wire, not the scheme to defraud." The Second Circuit in *Bascuñán v. Elsaca*, 927 F.3d 108 (2019), established a two-part framework requiring that "wire fraud involves sufficient domestic conduct when (1) the defendant used domestic mail or wires in furtherance of a scheme to defraud; and (2) the use of the mail or wires was a core component of the scheme to defraud."

These extraterritoriality determinations directly impact state court jurisdiction over related state law claims. When federal wire fraud claims establish domestic conduct sufficient to support federal jurisdiction, state courts often exercise supplemental jurisdiction over related state law claims, applying their choice of law analysis to determine which state's law governs these ancillary claims.

Best Practices to Prevent Wire Fraud

Education is key (and your insurer may require it)

Ongoing education is essential. Conduct regular training on email scams and wire transfer best practices, and foster a culture of verification and communication throughout the organization.

Train Your Employees: Your best defense against wire fraud is an informed staff. Employees should never send passwords or sensitive information via email, even if the message appears to come from a manager. It is essential to explain common scam tactics and encourage employees to verify suspicious requests with coworkers or supervisors. Providing educational resources, such as the FTC brochure available at ftc.gov/bulkorder, will further strengthen awareness and preparedness.

Verify Invoices and Payments: Businesses must establish clear procedures for approving purchases and invoices. Staff should scrutinize all invoices for accuracy and pay close attention to payment methods. If someone insists on payment via wire transfer, cryptocurrency, or gift cards, it is almost certainly a scam. Implementing dual control and segregation of duties for payment approvals adds an extra layer of security.

Spot Tech-Related Scams: Technology-related scams are increasingly common. Caller ID cannot be trusted because scammers can spoof numbers. Employees should avoid clicking links, opening attachments, or downloading files from unexpected emails or texts. Social media account hacks can also lead to fraudulent messages that appear legitimate. Reviewing resources like Cybersecurity for Small Business can help organizations stay informed and protected.

Know Who You're Dealing With: Before engaging with a new company, search its name online along with terms like 'scam' or 'complaint' and read reviews. Always verify wire transfer requests by calling the requester using a previously verified phone number, not one provided in the email. Implementing a call-back verification process for new vendors or changes to payment instructions is critical.

Strengthen Internal Controls: Internal controls are vital to preventing fraud. Require dual authorization for wire

transfers and ensure duties are segregated so no single employee controls the entire payment process. Regularly test your fraud health and review procedures to maintain strong defenses. Check wire instructions by calling a phone number on file or publicly available for the alleged recipient.

Cybersecurity and Insurance: Implement and regularly update a cybersecurity policy to protect systems and data. Additionally, review your business insurance policy to confirm it covers financial losses resulting from cyber fraud.

Plan Your Response, and Test Your Plan

Incident Response Plan (Wire Fraud): An effective incident response plan defines leadership roles, actions required before returning to normal operations and establishes incident categories and severity levels. It should set clear response times and escalation procedures. The plan must address each stage of the incident-response life cycle: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-incident Activity. Procedures should include detection and reporting through a single hotline or email, immediate escalation to the Incident Response Lead, and defined response times such as responding to critical incidents within 15 minutes and notifying executives within 30 minutes. Assessment involves triage and forensic data collection, including email headers and logs. The plan should list contacts such as law enforcement, legal counsel, cyber insurance providers, banks, vendors, and members of the incident response team. Operating procedures must cover containment, remediation, and post-incident activities, including system quarantine, disaster recovery, business continuity, and feedback loops to strengthen processes. Annual testing through tabletop exercises or simulated attacks ensures readiness.

Investigate and Notify Banking Partners and Law Enforcement

Investigation: When fraud is discovered, act quickly and gather as much information as possible. Pinpoint when the fraud occurred, determine who authorized the transactions, establish how many times the fraud happened, calculate the total value, and identify who validated the transactions. Forensic steps include collecting email headers, system logs, IP addresses, and device identifiers while preserving evidence with legal holds and chain of custody. Notifications should include contacting banking partners immediately to request recalls or holds, reporting via IC3.gov, and requesting Financial Fraud Kill Chain support if eligible. Notify your cyber insurance provider and involve legal counsel to meet regulatory and contractual requirements.

Remediate Appropriately

Remediation and Recovery: Containment measures include disabling compromised accounts, enforcing multi-factor authentication, blocking malicious domains and IPs, removing auto-forwarding rules, and halting pending payments until re-verified. Eradication involves malware scans, reimaging affected systems, auditing mailboxes and security controls, and validating vendor master changes through out-of-band verification. Recovery steps include restoring services incrementally, monitoring for recurrence, reconciling financial accounts, and documenting residual losses. Engage third-party digital forensics and incident response specialists if needed and leverage cyber insurance resources. Finally, develop an After Action Report to document timelines, decisions, outcomes, and lessons learned. Assign remediation owners with deadlines, update policies and training, and schedule follow-up audits and tabletop exercises.