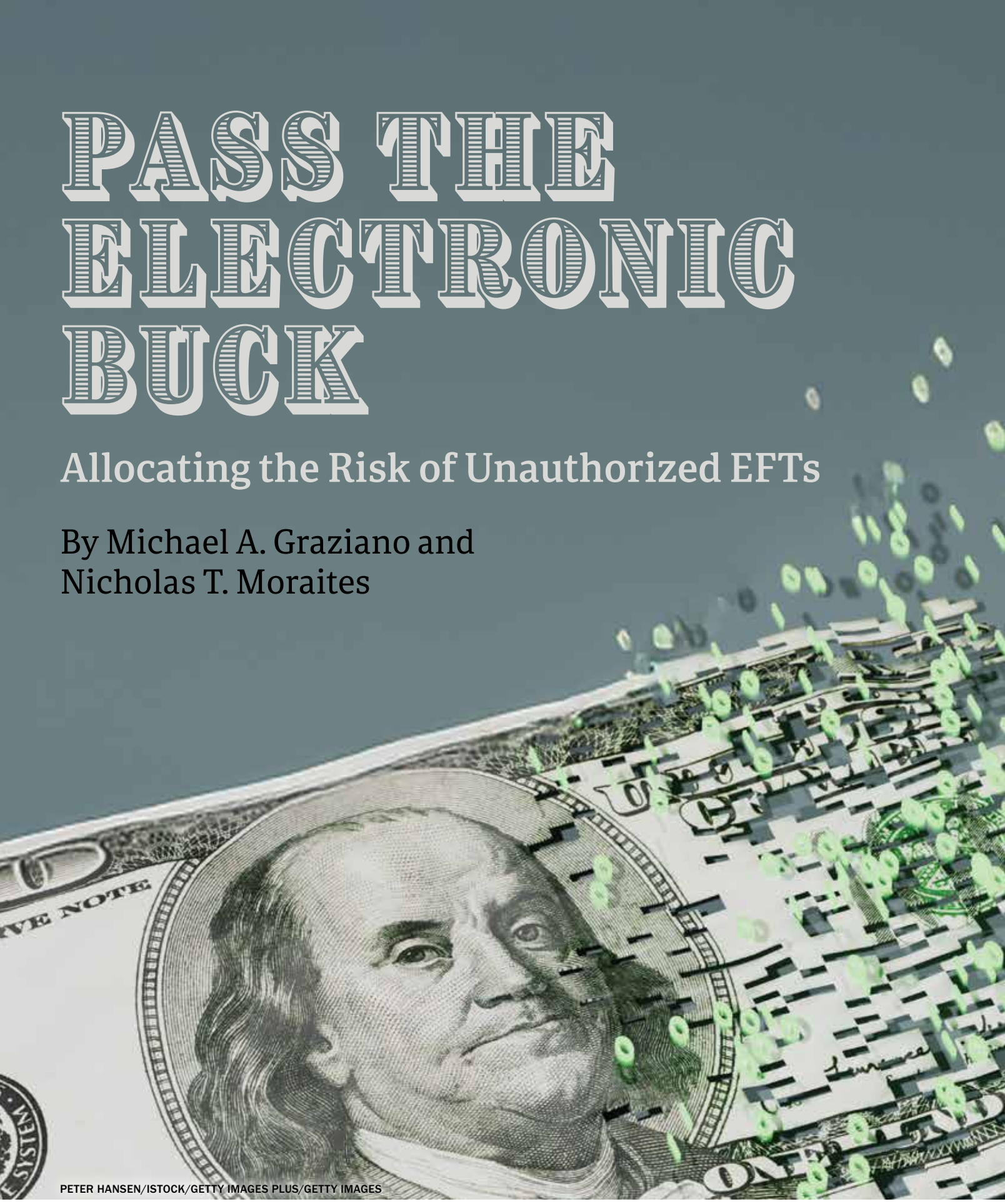
PASS THE ELECTRONIC BUCK

Allocating the Risk of Unauthorized EFTs

By Michael A. Graziano and Nicholas T. Moraites



PETER HANSEN/ISTOCK/GETTY IMAGES PLUS/GETTY IMAGES

From small consumer transactions to large commercial deals, the modern economy runs on electronic funds transfers (EFTs). The technology and controls used to effectuate EFTs in a secure manner are constantly evolving, but bad actors are never far behind when it comes to finding ways to disrupt the system and steal money. According to the FBI, the public reported $12.5 billion in losses from cybercrimes during 2023 alone.[1] That figure may be just the tip of the iceberg.

When an unauthorized, or fraudulently induced, EFT occurs, which of the innocent parties involved in the failed transaction is left holding the proverbial bag? Courts are increasingly faced with that question, but the answer is not always clear. It often requires analyzing a complex web of obligations created by private contracts, federal and state statutes and regulations, and long-standing common law principles.

What Is an EFT and Who Is Involved?

In its broadest sense, an EFT can be viewed as any exchange of funds through technology. Examples can range from wire transfers transacted through a Federal Reserve Bank or transfers through the Automated Clearing House (ACH), both of which are used by large businesses and individual consumers alike, to more consumer-oriented transactions such as point-of-sale credit or debit card transactions, or peer-to-peer transfers where neither the payor nor the payee is a sophisticated business entity. Different laws apply to different types of EFTs; and in some cases, the applicable law depends on whether an individual consumer is involved.

A typical EFT appears to be a simple bilateral transaction between a payee and a payor but is often much more complex and can involve numerous companies and financial institutions. A good example can be found in *RealPage, Inc. v. National Union Fire Insurance Co. of Pittsburgh*. The case arose from a dispute over insurance coverage for a phishing scheme that targeted an employee of a fintech company, RealPage, that helped facilitate payments but did not actually handle the funds.[2]

On the surface, the transactions at issue in *RealPage* appear to be simple rent payments from tenants. In reality, however, at least five steps were required for each rent payment.[3] First, the tenant entered banking information into an online platform maintained by RealPage. Second, RealPage provided the information and instructions to a third-party payment processor, Stripe. Third, Stripe instructed its bank to pull funds from the tenant's bank and transfer those funds into Stripe's bank account. Fourth, after deducting its own fees, Stripe instructed its bank to transfer funds to another bank to cover RealPage's fees, and to then transfer the remaining funds to the property manager's bank. Fifth, the property manager presumably instructed its bank to transfer the amount due to the property owner to that entity's bank. In the ordinary course of business, therefore, each rent payment involved a minimum of 10 parties: (1) the tenant; (2) the tenant's bank; (3) a tech company that maintained an online platform to facilitate the exchange of information, RealPage; (4) RealPage's bank; (5) a payment processor, Stripe; (6) the payment processor's bank; (7) the property manager; (8) the property manager's bank; (9) the property owner; and (10) the property owner's bank.[4]

A RealPage employee unwittingly provided credentials to a fraudster who used the credentials to pose as an authorized representative of RealPage and instruct Stripe to transfer funds to the fraudster's account. RealPage reimbursed the property managers and sought coverage under a commercial crime policy. The U.S. Court of Appeals for the Fifth Circuit held that the stolen funds did not qualify as covered property under the policy, however, because RealPage did not own, lease, or hold the funds at the time that the loss occurred.[5]

The Fifth Circuit's holding makes sense because RealPage itself did not handle any funds (at least until it collected its own fees); it simply facilitated the exchange of information. The holding in *RealPage* also highlights some of the questions an organization must ask when a loss occurs. Who did own the funds at the time of the loss at issue in *RealPage*? Who was holding the funds at the time of the loss? Who was otherwise responsible, or legally liable, for the funds at the time of the loss? Did RealPage owe contractual, statutory, or common law duties to any of those entities? If so, did RealPage breach those duties, and was any such breach the cause of the loss? Did any of those entities have viable claims against RealPage for the loss? Did they have viable claims against each other? Did any of the other parties have potentially applicable insurance coverage? Would the answer to any of those questions change if the fraudster also duped, or hacked, any of the nine other parties in addition to duping an employee of RealPage?

A prudent organization will anticipate these questions and ensure that its internal controls, standard contractual agreements, and insurance portfolio are designed to prevent losses where possible and transfer as much of the remaining risk as it can to counterparties and insurance carriers. Below are brief overviews of some of the potentially relevant legal authorities and risk mitigation strategies, but each situation is unique.

The Electronic Fund Transfer Act

The Electronic Fund Transfer Act (EFTA) is a federal statute that was adopted in 1978 and applies to certain types of EFTs.[6] EFTA's implementing regulation, which was issued by the Board of Governors of the Federal Reserve System, is commonly referred to as "Regulation E."[7] When EFTA is potentially implicated, the most difficult question is often whether it does or does not apply to the relevant transaction.

In analyzing whether EFTA applies, it is necessary to consider the statute as a whole because it contains precise definitions that may seem counterintuitive and that narrow the scope of EFTA's coverage in several important ways. For example, EFTA defines the term "account" as:

> a demand deposit, savings deposit, or other asset account (other than an occasional or incidental credit balance in an open end

TIP: Internal controls such as callback verifications and multilevel approvals not only prevent loss but also can prevent liability from attaching if a loss occurs.

> credit plan as defined in section 1602(i) of this title), as described in regulations of the Bureau, established primarily for personal, family, or household purposes, but such term does not include an account held by a financial institution pursuant to a bona fide trust agreement.[8]

As a result, EFTA applies only to consumer accounts used primarily for personal, family, or household purposes, and it does not apply to business accounts.[9]

Several types of transactions that may commonly be understood as EFTs are also excluded from EFTA's definition of "electronic fund transfer" even if they involve consumer accounts.[10] For example, EFTA does not apply to "the purchase or sale of securities or commodities through a broker-dealer," automatic transfers "for the purpose of covering an overdraft or maintaining an agreed upon minimum balance," or certain transfers that are "initiated by a telephone conversation between a consumer and an officer or employee of a financial institution."[11]

One significant exception to EFTA's coverage applies to

> any transfer of funds, other than those processed by automated clearinghouse, made by a financial institution on behalf of a consumer by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer.[12]

Many courts have held that the exception applies to all wire transfers.[13] In *New York ex rel. James v. Citibank, N.A.*, however, the U.S. District Court for the Southern District of New York held that the exception applies only to interbank transfers using a wire transfer system, and that the exception does not apply to the initial request by a consumer (or an imposter) to wire funds to a third party, including the consumer's payment to its own financial institution to cover the transfer.[14]

Setting aside any debate over whether *New York ex rel. James* reached the correct conclusion, its rationale, like the analysis in *RealPage*, demonstrates the importance of understanding the precise manner in which a transaction is effectuated as well as the role of each entity involved in the process. It is easy to overlook individual steps in what facially appears to be a simple transaction, but those nuances can be critical in answering questions as fundamental as whether EFTA or another body of law even applies to a transaction in the first place.

EFTA also defines the term "unauthorized electronic fund transfer" in a manner that excludes certain types of unauthorized transactions.[15] The definition applies to transactions "initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit," but it also contains express carve-outs.[16] For example, a transfer that is unauthorized will nevertheless be excluded from the definition if the consumer furnished the unauthorized party with the means to access the account and did not notify the financial institution that the third party was no longer authorized to access the account.[17]

At first blush, the carve-out appears to exclude unauthorized transfers caused by phishing and other social engineering schemes from the scope of EFTA because the hallmark of such schemes is a third party duping the victim into voluntarily authorizing a transfer or providing the means to do so. Some courts, however, have deferred to interpretations by federal regulators and applied a so-called "fraud exception" in holding that "[a]n unauthorized [electronic funds transfer] includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery."[18] In the wake of the U.S. Supreme Court's recent decision in *Loper Bright Enterprises v. Raimondo*,[19] courts may give less deference in future cases to federal regulators in considering whether EFTA applies when a consumer voluntarily provides means of access to a fraudster.

When EFTA does apply, its application is fairly straightforward because it does not require weighing blameworthiness. Instead, EFTA establishes strict limitations on a consumer's liability for unauthorized transactions provided that the consumer gives notice in a timely manner.[20] Specifically, EFTA "presumptively caps consumer liability for 'unauthorized' transfers at $50."[21] A financial institution is not required to reimburse the consumer, however, if it establishes that a loss "would not have occurred but for the failure of the consumer" to provide notice within 60 days of receiving the account statement listing the unauthorized transaction.[22] A different timeline applies if the transaction involved the loss or theft of a card or other access device.[23]

The fact that EFTA is limited to consumers does not mean that it can always be ignored in analyzing commercial losses, especially when a fintech company is the target of a fraud scheme. For example, although the fraudster in *RealPage*

Michael A. Graziano *is a member in the Washington, D.C., office of Eckert Seamans Cherin & Mellott, LLC. He focuses his practice on commercial litigation with an emphasis on fidelity and crime insurance and financial services litigation. He is a regular contributor to conferences and publications in the fidelity and crime insurance industry. He may be reached at mgraziano@eckertseamans.com.*
Nicholas T. Moraites *is assistant vice president, claims, in Great American Insurance Company's Fidelity/Crime Division. He has more than 15 years of fidelity coverage/claims experience, including time at another fidelity/crime carrier and in private practice. He may be reached at nmoraites@gaig.com.*

targeted transactions between a fintech company and a payment processor, the stolen funds may have originated in consumer accounts if the underlying leases were residential rather than commercial. If so, it begs the question: Would a court have held that EFTA capped the tenants' liability at $50 per transaction and required their banks to reimburse the tenants for the remainder of the losses so that they could make their rent payments?

Of course, even if the tenants were entitled to reimbursement from their banks under EFTA, it does not mean that those banks would be left without recourse against the other entities involved in the transactions. Since those entities were not individual consumers, however, any such recourse likely would not be governed by EFTA.

Article 4A of the Uniform Commercial Code

The Uniform Commercial Code (UCC) establishes a uniform set of rules to "simplify, clarify, and modernize the law governing commercial transactions" on a nationwide basis.[24] The UCC itself does not have the force of law, but all 50 states and the District of Columbia have adopted at least some of its provisions. As such, in applying the UCC to real-world issues, it is necessary to consult the version of the UCC that was adopted by the relevant state.

Funds transfers are addressed in Article 4A of the UCC.[25] The UCC defines "funds transfer" as "the series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order."[26] It also includes intermediary payment orders necessary to carry out the originator's instruction.[27]

Significantly, EFTA and Article 4A are not designed to overlap.[28] The UCC expressly states that it "does not apply to a funds transfer any part of which is governed by the Electronic Fund Transfer Act of 1978."[29] If the holding in *New York ex rel. James* that EFTA can apply to certain transactions that are incidental to a wire transfer becomes widely accepted, an unintended consequence may be the removal of certain aspects of wire transfers involving individual consumers from the scope of Article 4A.[30]

Unlike EFTA, Article 4A does not focus narrowly on the relationship between a bank and its account holder. Instead, Article 4A establishes rules of engagement for all parties directly involved in a funds transfer.[31] The UCC uses various designations to refer to a party based on the role it plays in a particular transfer instead of based on any fixed characteristics of that party. For example, in any given transaction, a bank could be referred to as the "receiving bank," the "originator's bank," the "beneficiary's bank," an "intermediary bank," or a combination thereof.[32] If the bank is actually a party to the underlying transaction, it could serve another role as well.[33] In fact, the definition of "customer" expressly states that it "includ[es] a bank."[34] The rights and obligations of the parties vary significantly depending on which designation applies, so it is critical to analyze that issue before applying the substantive provisions of Article 4A.

Despite its broad applicability to the parties directly involved in a funds transfer, Article 4A does not necessarily apply to fintech companies that do not actually handle funds. As previously explained, a "funds transfer" is defined as "the series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order."[35] Article 4A may not apply, therefore, to actions taken by a fintech company that simply facilitates the flow of information without submitting a payment order directly to a bank, and without holding funds in an account that the fintech company itself owns or controls, as was the case in *RealPage*.

Parts 2 through 5 of Article 4A establish the obligations of the parties involved in a particular funds transfer. A detailed description of those obligations is outside the scope of this article, but one particular provision, section 4A-207, is worth noting because it has created a significant amount of controversy when it comes to analyzing the allocation of liability following an unauthorized transfer.

EFTA defines the term "unauthorized electronic fund transfer" in a manner that excludes certain types of unauthorized transactions.

Section 4A-207 applies when a payment order misdescribes the beneficiary such that the identity of the intended beneficiary is not clear.[36] Under subsection (a), the payment order cannot be accepted if the "identification of the beneficiary refers to a nonexistent or unidentifiable person or account."[37] The remainder of section 4A-207 addresses circumstances in which inconsistent identifying information is provided—for example, when a payment order includes an account number and a name, but the name does not correspond to the account number.[38] "[I]f the beneficiary's bank does not know that the name and number refer to different persons, it may rely on the number," and the bank does not need to determine whether the name and number refer to the same person.[39]

The U.S. Court of Appeals for the Fourth Circuit recently analyzed section 4A-207 in *Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union*.[40] In that case, the victim

of a social engineering scheme alleged that a credit union violated section 4A-207, as adopted by Virginia, when it accepted payment orders despite having received automated reports noting a mismatch between the account number and the name of the intended beneficiary.[41] The trial court held that the credit union could be "imputed" with knowledge of the misdescription based on a general provision of the UCC stating that "[a]n organization has actual knowledge for a particular transaction 'from the time it would have been brought to the individual's attention if the organization had exercised due diligence.'"[42] After a bench trial, the court found that the credit union did not exercise due diligence.[43]

The credit union appealed, and the case garnered attention from several trade associations as well as the organization that governs the ACH system, the National Automated Clearing House Association (NACHA), all of whom filed amicus curiae briefs. The Fourth Circuit reversed the trial court's decision and held that, for purposes of section 4A-207, "'"[k]nowledge" means actual knowledge,' not imputed knowledge or constructive knowledge."[44] Since no individual employee of the credit union had reviewed the automated reports, the credit union did not have actual knowledge of the misdescription and, therefore, was not liable.[45] In explaining its rationale, the Fourth Circuit noted that requiring individualized review of all mismatches "would be most impractical, time-consuming, and expensive and would impede the efficient transfer of funds, imposing gridlock on the financial system."[46]

At least six courts have held that the payor bore the risk of loss because it failed to call the payee to verify wire instructions before initiating the wire transfer.

Interestingly, Judge Wynn authored a separate opinion that raises an important question about what qualifies as "actual knowledge" for purposes of section 4A-207. The opinion, which concurred with the judgment on different grounds, agrees with the majority's holding that "the actual knowledge requirement means that an 'individual' employee at the bank must have actual knowledge of the misdescription at the time of deposit."[47] The concurring opinion argues, however, that a fact finder could have determined that the credit union had actual knowledge of the misdescription because a credit union employee may have reviewed the automated reports while investigating a different issue.[48] That argument raises an important question: Does "actual knowledge" require that an individual employee actually understood and appreciated the contents of a report, or is it sufficient for the plaintiff to prove that an employee glanced at the report? The answer could prove to be critical in future cases.

As the Fourth Circuit and others have pointed out, requiring financial institutions to conduct an individual review of every payment order would be costly and unwieldy and could cause significant disruptions to the financial system. While those concerns are valid and important, so too is the need to prevent losses caused by social engineering and other fraud schemes carried out by imposters. In any event, time will tell whether section 4A-207 will ultimately prove to be a generally accepted method for allocating the risk of loss from such schemes.

The Imposter Rule

Since 2015, a growing number of courts have adopted a test known as the "imposter rule" in analyzing which party should bear the risk of loss for a social engineering scheme.[49] The trend appears to have started with *Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment, Inc.*[50] In that case, a purchaser was duped into sending a payment via wire transfer based on wire instructions it received from a fraudster who impersonated the seller.[51] The court drew an analogy between the social engineering scheme and check forgery, and it cited "cases in the banking context dealing with third party 'imposters' and forged checks that are helpful to resolve this issue."[52] The imposter rule, at least as applied to check forgery, is derived from section 3-404(d) of the UCC.[53]

"Under the 'imposter rule,' the party who was in the best position to prevent the forgery by exercising reasonable care suffers the loss."[54] Applying that rule to the unauthorized wire transfer at issue in *Arrow Truck Sales*, the court held that the purchaser was in the best position to prevent, and was therefore required to bear, the loss because the purchaser likely could have thwarted the scheme by simply calling the seller to verify the new wire instructions before initiating the wire transfer.[55]

A few courts have expressed doubt as to whether the imposter rule should even apply to EFTs, and at least one court expressly declined to apply it.[56] As its critics correctly point out, the imposter rule is a creature of statute that does not, at least on its own terms, apply to EFTs because Article 3 of the UCC governs negotiable instruments, whereas funds transfers are governed by Article 4A.[57] Nevertheless, the majority of courts that have considered the issue have applied the imposter rule to EFTs in some form or another.[58]

From a procedural standpoint, the imposter rule requires a fact-intensive balancing of various factors. As a result, summary judgment may be difficult to obtain, and many of the opinions that weigh the relevant factors involved bench trials

or motions to enforce settlement agreements.[59] Some courts have expressly held that the issue could not be resolved on summary judgment.[60] At least one court, however, did resolve the issue on summary judgment.[61]

There is no agreed-upon set of elements or factors that courts weigh in applying the imposter rule. The *Galaxy International, Inc. v. Merchants Distributors, LLC*, opinion, however, provides a helpful list of the types of factors that might be relevant (although the court ultimately did not apply the rule).[62] The court explained that the following questions may be pertinent: "whether [the payee] had sufficient security protecting its email system from being hacked or not"; "when [the payee] knew or should have known that [its] email had been hacked"; "if [the payee] acted reasonably when it did not alert [the payor] that [its] email had been hacked and had sent out fraudulent ACH instructions to another customer"; "whether [the payor's] employees should have verified the ACH instructions with [the payee] prior to making the ACH payment"; "if [the payor] had an internal policy requiring verification of ACH instructions and the scope of such policy"; and "whether [the payor's] internal policy and actions were reasonable given the company's awareness of an ACH fraud scheme involving [a] related entity."[63]

One factor stands out as having proved dispositive in more cases than the other factors combined: the callback verification. At least six courts have held that the payor bore the risk of loss because it failed to call the payee to verify wire instructions before initiating the wire transfer.[64] Another factor that has been afforded significant weight is a party's prior knowledge of a known risk, such as, for example, knowledge of an incident in which the same imposter used a fake email account in connection with a prior, unrelated transaction.[65] The payee in *Bile v. RREMC, LLC*, was aware of such a risk, and the court held that the payee's failure to inform the counterparty meant that the payee should bear the risk of loss.[66]

Another issue that frequently arises occurs when a hacker infiltrates a party's computer system. That fact will not necessarily be dispositive, however, especially when the counterparty falls victim to social engineering.[67] In *Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, the payee's email account was hacked by the fraudster, but the court held that a triable issue existed because a fact finder could conclude that the payor was in a better position to prevent the loss because the payor relied on suspicious wire instructions.[68]

Common Law and Private Contracts

In addition to federal and state statutes, the parties involved in an EFT may owe relevant duties to each other under the common law or private contracts. Many tort claims may be displaced by statutes, or barred by the economic loss doctrine, but the common law claims that are viable will likely vary significantly from one jurisdiction to another.[69]

Some courts have found well-established common law principles to be helpful in determining who should bear the risk of loss for an unauthorized EFT. In particular, some courts have cited general principles of contract and agency law that are consistent with the imposter rule because they focus on identifying the party who was in the best position to prevent the fraud.[70] For example, a party to a contract bears the risk of a mistake if, among other reasons, "the risk is allocated to him by the court on the ground that it is reasonable in the circumstances to do so."[71] In many, if not all, circumstances, that principle and the imposter rule will lead to the same result because it is "reasonable" to allocate the risk of loss to the party that was in the best position to prevent it.

General principles of agency law can also be helpful. Specifically, a person may be liable for the acts of an imposter if that person "intentionally or carelessly" caused a third party to believe that the imposter had authority, or, "having notice of such belief and that it might induce others to change their positions, the person did not take reasonable steps to notify them of the facts."[72] As previously explained, courts have considered those same factors in applying the imposter rule.[73]

The express or implied terms of private contracts may also shift the risk of loss between the contracting parties. For example, companies that regularly exchange funds for goods on a large scale could include provisions requiring each other to employ certain controls to prevent social engineering losses, to safeguard financial and other confidential information, to provide indemnification against losses in certain circumstances, or a combination thereof. If so, the relevant contractual provisions may trump the general common law principles discussed above. Furthermore, contracts between and among the banks involved in an EFT, and their respective customers, may also contain relevant provisions.

Finally, it may also be necessary to consider rules that govern payment systems generally. For example, as a condition to participating in ACH transactions, financial institutions may agree to be bound by the rules adopted by NACHA. Many financial institutions incorporate those rules into their standard account agreements. As a result, some or all parties to an EFT may be bound by the NACHA rules in addition to any other applicable contracts.

Risk Mitigation

When it comes to EFTs, the most important way to mitigate risk is by adopting and following internal controls designed to prevent unauthorized transactions. Internal controls such as callback verifications and multilevel approvals not only prevent loss but also can prevent liability from attaching if a loss occurs, especially in jurisdictions that apply the imposter rule. It is also essential for organizations to adopt robust data security measures for the same reasons.

Of course, no internal controls are foolproof. It is also important, therefore, for an organization to consider options to transfer risk. An organization can reduce its exposure by including provisions in standard contracts that require counterparties to adopt their own internal controls, to safeguard financial and

other confidential information, to provide indemnification in the event that a loss occurs, or all of the above.

An organization should also evaluate its insurance portfolio to make sure that it has obtained appropriate coverage. There are several products available in the market that provide coverage for losses involving unauthorized EFTs under certain circumstances. For example, insuring provisions applicable to funds transfer fraud, fraudulently induced transfers, social engineering, and similar risks are included in some standard crime policies or may be offered in riders or endorsements for an additional premium. Similar provisions are also sometimes added to cyber policies.

If a company has a potentially applicable insurance policy, it must also ensure that it is employing any internal controls that are a condition precedent to coverage. For example, many standard policy forms require the insured to perform a callback verification to a predetermined phone number before initiating a wire transfer as a condition precedent to coverage attaching to a loss caused by a fraudulently induced transfer.

Final Thoughts

Neither EFTs nor the risk of loss from unauthorized EFTs is going anywhere anytime soon. To prevent losses involving EFTs, and to avoid being held liable when a loss does occur, organizations should be aware of the internal controls and legal principles courts have considered in analyzing who bears the risk of loss. When a loss occurs, an organization must act quickly to notify the relevant parties, attempt to recover the loss, and evaluate its options based on the complex web of laws and contracts that may apply. ◀

Notes

1. Internet Crime Complaint Ctr., Fed. Bureau of Investigation, 2023 Internet Crime Report (2024), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.
2. 21 F.4th 294 (5th Cir. 2021).
3. *Id.* at 296–97.
4. *Id.*
5. *Id.*
6. 15 U.S.C. §§ 1693 *et seq.*
7. 12 C.F.R. § 1005.
8. 15 U.S.C. § 1693a(2).
9. *See id.*
10. *Id.* § 1693a(7).
11. *Id.*
12. *Id.* § 1693a(7)(B).
13. *See, e.g.*, Nazimuddin v. Wells Fargo Bank, N.A., No. 24-20343, 2025 WL 33471, at *2 (5th Cir. Jan. 6, 2025).
14. No. 24-CV-659 (JPO), 2025 WL 251302, at *5–14 (S.D.N.Y. Jan. 21, 2025).
15. 15 U.S.C. § 1693a(12).
16. *Id.*
17. *Id.*
18. Green v. Cap. One, N.A., 557 F. Supp. 3d 441, 447 (S.D.N.Y. 2021) (alterations in original) (quoting 12 C.F.R. pt. 205, Supp. I at 2(m) (Board of Governors' official interpretation of § 205.2(m)); 12 C.F.R. pt. 1005, Supp. I at 2(m) (Consumer Financial Protection Bureau's official interpretation of § 1005.2(m))); Georgion v. Bank of Am., N.A., No. 3:22-CV-00618-RJC-WCM, 2024 WL 3844960, at *5 (W.D.N.C. Mar. 20, 2024).
19. 603 U.S. 369 (2024).
20. *See* 15 U.S.C. § 1693g.
21. *Green*, 557 F. Supp. 3d at 446; 15 U.S.C. § 1693g(a).
22. 15 U.S.C. § 1693g(a).
23. *Id.*
24. U.C.C. § 1-103(a)(1) (Am. L. Inst. & Unif. L. Comm'n 2012).
25. *Id.* § 4A-102.
26. *Id.* § 4A-104(a).
27. *Id.*
28. *Id.* § 4A-108(a).
29. *Id.*
30. *See* No. 24-CV-659 (JPO), 2025 WL 251302, at *5–14 (S.D.N.Y. Jan. 21, 2025).
31. U.C.C. §§ 4A-103, -104.
32. *Id.*
33. *Id.*
34. *Id.* § 4A-105(3).
35. *Id.* § 4A-104(a).
36. *Id.* § 4A-207.
37. *Id.* § 4A-207(a).
38. *Id.* § 4A-207(b)–(d).
39. *Id.* § 4A-207(b)(1).
40. *Studco II*, 133 F.4th 264, 267 (4th Cir. 2025).
41. *Id.* at 268–72.
42. Studco Bldg. Sys. US, LLC v. 1st Advantage Fed. Credit Union (*Studco I*), No. 2:20-CV-417, 2023 WL 1926747, at *13–14 (E.D.Va. Jan. 12, 2023) (citing Va. Code Ann. § 8.1A-202(f)).
43. *Id.*
44. *Studco II*, 133 F.4th at 273 (quoting Va. Code Ann. § 8.1A-202(b)).
45. *Id.* at 275.
46. *Id.* at 274.
47. *Id.* at 277–78 (Wynn, J., concurring in part).
48. *Id.*
49. *See, e.g.*, Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc., No. 8:14-CV-2052-T-30TGW, 2015 WL 4936272 (M.D. Fla. Aug. 18, 2015).
50. *See id.*
51. *Id.* at *1–4.
52. *Id.* at *5.
53. *Id.* (citing U.C.C. § 3-404(d)).
54. *Id.*
55. *Id.* at *6.
56. Peeples v. Carolina Container, LLC, No. 4:19-CV-21-MLB, 2021 WL 4224009, at *7 (N.D. Ga. Sept. 16, 2021) (declining to apply the imposter rule); Galaxy Int'l, Inc. v. Merchs. Distribs., LLC, No. 22-302, 2023 WL 4949864, at *2 (W.D. Pa. Aug. 3, 2023); Kenwell Trading Ltd. v. Porcelen Ltd. CT LLC, No. 3:22-CV-00248 (KAD), 2022 WL 3359159, at *4 (D. Conn. Aug. 15,

2022); *see also* TMX Constr. v. Revolution Pipeline, LLC, 540 P.3d 1096, 1102–03 (Okla. Civ. App. 2023) (Blackwell, J., dissenting).

57. *Peeples*, 2021 WL 4224009, at *7.

58. *Arrow Truck Sales*, 2015 WL 4936272; Bile v. RREMC, LLC, No. 3:15CV051, 2016 WL 4487864 (E.D.Va. Aug. 24, 2016); Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc., 759 F. App'x 348 (6th Cir. 2018); Jetcrete N. Am. LP v. Austin Truck & Equip., Ltd., 484 F. Supp. 3d 915 (D. Nev. 2020); Parmer v. United Bank, Inc., No. 20-0013, 2020 WL 7232025 (W.Va. Dec. 7, 2020); Mile High, LLC v. Flying M Aviation, Inc., No. CL-2023-0260, 2024 WL 57451 (Ala. Civ. App. Jan. 5, 2024); Forde v. Krantz, No. 21-CV-80603-RKA, 2023 WL 7109745 (S.D. Fla. Oct. 27, 2023); *TMX Constr.*, 540 P.3d 1096; Ostrich Int'l Co., Ltd. v. Michael A. Edwards Grp. Int'l Inc., No. 2:21-CV-00639-JVS(ASx), 2023 WL 4025870 (C.D. Cal. May 18, 2023).

59. *See Galaxy Int'l*, 2023 WL 4949864; *Beau Townsend*, 759 F. App'x 348; *TMX Constr.*, 540 P.3d 1096.

60. *See supra* note 59.

61. *Forde*, 2023 WL 7109745.

62. 2023 WL 4949864, at *3–4.

63. *Id*.

64. Ostrich Int'l Co., Ltd. v. Michael A. Edwards Grp. Int'l Inc., No. 2:21-CV-00639-JVS(ASx), 2023 WL 4025870 (C.D. Cal. May 18, 2023); Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc., No. 8:14-CV-2052-T-30TGW, 2015 WL 4936272 (M.D. Fla. Aug. 18, 2015); Jetcrete N. Am. LP v. Austin Truck & Equip., Ltd., 484 F. Supp. 3d 915 (D. Nev. 2020); Parmer v. United Bank, Inc., No. 20-0013, 2020 WL 7232025 (W.Va. Dec. 7, 2020); *Forde*, 2023 WL 7109745; Mile High, LLC v. Flying M Aviation, Inc., No. CL-2023-0260, 2024 WL 57451 (Ala. Civ. App. Jan. 5, 2024).

65. Bile v. RREMC, LLC, No. 3:15CV051, 2016 WL 4487864 (E.D.Va. Aug. 24, 2016).

66. *Id*.

67. Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc., 759 F. App'x 348 (6th Cir. 2018).

68. *Id*.

69. *See generally* Russell Barnett Ford of Tullahoma, Inc. v. H & S Bakery, Inc., 398 F. Supp. 3d 287 (E.D. Tenn. 2019) (common law negligence claims were displaced by the UCC).

70. *See, e.g.*, *Beau Townsend*, 759 F. App'x at 353–58.

71. Restatement (Second) of Contracts § 154 (Am. L. Inst. 1981).

72. Restatement (Third) of Agency § 2.05 (Am. L. Inst. 2006).

73. *See, e.g.*, Bile v. RREMC, LLC, No. 3:15CV051, 2016 WL 4487864 (E.D.Va. Aug. 24, 2016).