Technology and Salvage:
Using Social Media in Recovery and
Allocating Cybercrime Funds Transfers to Third Parties

January 31, 2020

American Bar Association ▪ Tort Trial & Insurance Practice Section
Fidelity and Surety Law 2020 Midwinter Conference

Robert W. Ludwig
Salvatore Scanio
Ludwig & Robinson PLLC
1717 Pennsylvania Ave., N.W.
Suite 450
Washington, DC 20006
(202) 289-1800

Joseph S. Szary
Great American Insurance Group
103 Carnegie Center
Suite 207
Princeton, NJ 08540
(609) 297-1407

I. INTRODUCTION

This paper analyzes how technology affects salvage in two ways. First, it addresses how social media may be used effectively in locating individuals and businesses, their income and assets, and covers applicable regulatory guidelines. Second, this paper discusses the latest trends in cybercrime involving fraudulent funds transfers and how losses are allocated between insureds and third-parties, particularly banks.

II. SOCIAL MEDIA IN RECOVERY

In today's society, social media is ubiquitous. As of the first quarter of 2019, the number of monthly active users for the major platforms was staggering: Facebook, 2.27 billion; YouTube 1.9 billion; Instagram, 1 billion; Twitter, 326 million; LinkedIn, 260 million; and Pinterest, 250 million.[1] Worldwide, there are approximately 3.4 billion social media users spending an average of 135 minutes per day on social media.[2] In the United States, 79% of the population, or 247 million people, own at least one social media profile.[3] The percentage of U.S. adults using social media by platform includes: 73% YouTube; 69% Facebook; 37% Instagram; 28% Pinterest; 27% LinkedIn; and 22% Twitter.[4]

Consequently, lawyers now regularly use social media in their cases. According to the ABA Legal Technology Survey Report, 30 percent of respondents used social media to investigate their cases.[5] In 2012, the ABA revised Comment 8 to Model Rule 1.1 to state that in order to

[1] StatusBrew, *100 Social Media Statistics for Businesses 2019* (Dec. 27, 2018), available at https://blog.statusbrew.com/social-media-statistics-2019 (last visited Nov. 18, 2019).

[2] *Id.*

[3] Statista, *Percentage of U.S. population with a social media profile from 2008 to 2019* (Aug. 9, 2019), available at https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/ (last visited Nov. 18, 2019).

[4] Pew Research Center, *Share of U.S. Adults Using Social Media, Including Facebook, is Mostly Unchanged Since 2018* (Apr. 10, 2019), available at https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/ (last visited Nov. 21, 2019).

[5] Nicole Black, *Lawyers and Social Media in 2019*, available at https://www.mycase.com/blog/2019/01/lawyers-and-social-media-in-2019/ (last visited Nov. 18, 2019).

"maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*."[6] Some commentators "believe that running a social media search of clients, opponents, and witnesses is now part of the minimum level of due diligence expected of a competent litigator."[7] One court quoted with approval a commentator's view that "It should be a matter of professional competence for attorneys to take the time to investigate social networking sites."[8]

A. Recovery Against Principals/Businesses

Social media contains a wealth of information, much of it publicly available. In pursuing recovery of a fidelity or commercial crime loss through subrogation and/or assignment, an insurer and its counsel may consider the utility of social media searches in locating assets, sources of income, and fraudulent transfers.

Social media sites may be searched individually or globally on the Internet to identify relevant user accounts. Technology firms offer services to search the Internet to identify social media accounts.[9] Technology firms also offer services to broadly search within major social media platforms, to capture relevant posts and available metadata, and to export such data to litigation document management programs.[10]

[6] ABA Model Rule 1.1, Comment 8 (emphasis added).

[7] Andy Radhakant & Matthew Diskin, *How Social Media Are Transforming Litigation*, 39 LITIGATION 17 (Spring 2013), at 18; *see also* ABA, *LITIGATION: How Social Media Are Transforming Litigation* (Apr. 10, 2019) (same), available at https://www.americanbar.org/groups/gpsolo/publications/gp_solo/2013/september_october/litigation_how_social_media_are_transforming_litigation/ (last visited Nov. 18, 2019).

[8] Griffin v. State, 995 A.2d 791, 801 (Md. Ct. Spec. App. 2010) (quoting Sharon Nelson, John Simek and Jason Foltin, *The Legal Implication of Social Networking*, 22 REGENT U.L. REV. 1, 14 (2009/2010)), *rev'd on other grounds*, 19 A.3d 415 (Md. 2011).

[9] For example, LexisNexis's Accurint service now includes a Social Media Locator feature. *See, e.g.*, *LexisNexis Expands Use of Social Intelligence Solution for Fraud Detection*, INSURANCE INNOVATION REPORTER (Feb. 1, 2016), available at http://iireporter.com/lexisnexis-expands-use-of-social-intelligence-solution-for-fraud-detection/ (last visited Nov. 19, 2019).

[10] For example, two firms providing these services are X1, *see* https://www.x1.com/products/x1-social-discovery/ (last visited Nov. 19, 2019), and Page Vault, *see* https://www.page-vault.com/ (last visited Nov. 19, 2019).

Some forms of research on social media sites are fairly obvious, such as reviewing LinkedIn for someone's latest employer or associated business or Facebook for where someone lives. Other forms of social media research can be more complex. For example, relationships with others can be discovered through their Facebook friends, Twitter followers, and the like. These other profiles can be searched to find mention of the relevant person, such as in an Instagram post, which could be useful in identifying where the person lives or in discovering fraudulent transfers to such friends. Review of who a user is following on Twitter or other social media may be helpful in locating assets, such as the identity of a financial institution followed by the user. The geolocation data found in images and other posts may be helpful in locating the user. Some social media platforms have features by which a user "checks-in" at a business or location. In all, review of social media can often provide insights into the user unavailable elsewhere, sometimes resulting in highly useful "smoking gun"-type information.

B. **Monitoring**

One common method of tracking someone on the Internet is to set up alerts. For example, Google Alerts "sends emails to the user when it finds new results—such as web pages, newspaper articles, blogs, or scientific research—that match the user's search term(s)."[11] There are also services available to monitor the Internet and major social media platforms.[12]

[11] WIKIPEDIA: THE FREE ENCYCLOPEDIA, entry of "Google Alerts," available at https://en.wikipedia.org/wiki/Google_Alerts (last visited Nov. 19, 2019).

[12] One such service is Mention. *See How to Use Mention App for Effective Web and Social Media Monitoring*, Razor Social, available at https://www.razorsocial.com/social-media-monitoring-tool-mention/ (last visited Nov. 19, 2019).

C. Regulatory Guidelines

1. Applicable to Industry

In December 2013, the Federal Financial Institutions Examination Council (FFIEC) issued guidelines governing social media use by banks, savings associations, and credit unions, as well as by nonbank entities supervised by the Consumer Financial Protection Bureau ("CFPB").[13] The guidance includes references to relevant law and regulations, some of which are generally applicable to industry, including the following:

> **Fair Debt Collection Practices Act.** The Fair Debt Collection Practices Act (FDCPA) restricts how debt collectors (generally defined as third parties collecting others' debts and entities collecting debts on their own behalf if they use a different name) may collect debts. The FDCPA generally prohibits debt collectors from publicly disclosing that a consumer owes a debt. Using social media to inappropriately contact consumers, or their families and friends, may violate the restrictions on contacting consumers imposed by the FDCPA. Communicating via social media in a manner that discloses the existence of a debt or to harass or embarrass consumers about their debts (e.g., a debt collector writing about a debt on a Facebook wall) or making false or misleading representations may violate the FDCPA.
>
> **Unfair, Deceptive, or Abusive Acts or Practices.** Section 5 of the Federal Trade Commission (FTC) Act prohibits "unfair or deceptive acts or practices in or affecting commerce." Sections 1031 and 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act prohibit unfair, deceptive, or abusive acts or practices. An act or practice can be unfair, deceptive, or abusive despite technical compliance with other laws. A financial institution should not engage in any advertising or other practice via social media that could be deemed "unfair," "deceptive," or "abusive." Of course, any determination as to whether an act or practice engaged in through social media is unfair, deceptive, or abusive, will necessarily be fact-specific. As with other forms of communication, a financial institution should ensure that information it communicates on social media sites is accurate, consistent with other information delivered through electronic media, and not misleading.
>
> . . .
>
> **CAN-SPAM Act and Telephone Consumer Protection Act.** The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) and Telephone Consumer Protection Act (TCPA) may be relevant if a financial institution sends unsolicited communications to consumers via social

[13] FFIEC, *Social Media: Consumer Compliance Risk Management Guidance* (Dec. 11, 2013).

> media. The CAN-SPAM Act and TCPA, and their implementing rules, establish requirements for sending unsolicited commercial messages ("spam") and unsolicited communications by telephone or short message service (SMS) text message, respectively.[14]

By way of example, the FTC asserts:

> [A] friend request that doesn't disclose that the "friend" reaching out to the consumer is really a debt collector would run afoul of the law. Debt collectors also shouldn't use social media to deceive third parties. A collector can't obtain location information about a consumer by using false pretenses to approach a friend or coworker – e.g., by using a fake Facebook account to send a friend request to a purported debtor's social connections in the hope of uncovering address or asset information.[15]

On May 21, 2019, the CFPB issued proposed amendments to Regulation F, implementing the Fair Debt Collection Practices Act, to prohibit debt collectors from contacting consumers through social media platforms except through a private messaging function.[16]

2. Applicable to Lawyers

"Lawyers, just like everyone else, are freely permitted to search social media for information concerning a litigant and to view the information that is generally available to the public."[17] "Finding and using . . . publicly available information" is appropriate, but "attempts to gain access to private social media accounts, blogs, and chat rooms are generally improper[,] includ[ing] the actions of third parties at the direction of the lawyer."[18] According to the Sedona Conference:

> Counsel may informally seek messages, posts, or other social media content, as the rules of professional conduct do not impose a blanket prohibition on such discovery. This occurs when social media content is available on sites, applications, or the internet without restrictions. In contrast, when relevant content is not readily

[14] *Id*. at 11, 15 (internal footnotes and citations omitted).

[15] FTC, *Debt collectors: You may "like" social media and texts, but are you complying with the law?* (Mar. 28, 2016), available at https://www.ftc.gov/news-events/blogs/business-blog/2016/03/debt-collectors-you-may-social-media-texts-are-you-complying (last visited Nov. 19, 2019).

[16] Debt Collection Practices (Regulation F), 84 Fed. Reg. 23274 (proposed May 21, 2019).

[17] John M. Flannery, *The Discoverability and Admissibility of Social Media in NY Civil Litigation*, in John M. Flannery *et al*., NEW DEVELOPMENTS IN EVIDENTIARY LAW IN NEW YORK 7, 11 (2013).

[18] Cheryl B. Preston, *Lawyers' Abuse of Technology*, 103 CORNELL L. REV. 879, 935-36 (May 2018).

> available without obtaining formal permission from the social media user, ethical violations can occur.[19]

One court and several bar associations have addressed the question of whether initiating a "friend" request to obtain non-publicly information is appropriate. In *Robertelli v. New Jersey Office of Atty. Ethics*,[20] the New Jersey Supreme Court held that the Office of Attorney Ethics could prosecute alleged misconduct involving attorneys who instructed a paralegal to send a "friend request" to the opposing party to monitor his Facebook account after it became private.[21] The opposing party's Facebook account was initially public, allowing the paralegal to access it, but she contacted the opposing party by way of the "friend request."[22] Although she used her own identity, she did not disclose that she worked for the law firm representing the defendants in the case.[23]

Further, the San Diego County Bar Association "concluded that the attorney's duty not to deceive prohibits him from making a friend request even of unrepresented witnesses without disclosing the purpose of the request."[24] Likewise, the Pennsylvania and New Hampshire bar associations have determined that viewing the public portions of a Facebook account is appropriate, but sending a "friend request" to access private information is inappropriate without using the lawyer's name and disclosing the purpose for the request.[25] The New York City Bar Association, however, reached a slightly different conclusion, finding "an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an

[19] The Sedona Conference, *Primer on Social Media*, 20 SEDONA CONF. J. 1, 91 (2d ed. 2019).
[20] 134 A.3d 963 (N.J. 2016).
[21] *Id*. at 975.
[22] *Id*. at 965.
[23] *Id*.
[24] San Diego County Bar Ass'n, Legal Ethics Op. 2011-2.
[25] Pa. Bar Ass'n Legal Ethics Comm., Op. 2014-300, at 8-9 (2014); N.H. Bar Ass'n Ethics Comm., Advisory Op. 2012-13/05, at 3.

unrepresented person's social networking website without also disclosing the reasons for making the request,"[26] provided the request does not include any misrepresentation.

III. Use of Technology to Investigate Cybercrime on the Dark Web

Cybercriminals conduct business on the dark web. A recent blog titled, "The Big Business of Cybercrime: The Dark Web," discusses how "Criminals have relied on the dark web to buy and sell all sorts of contraband – ranging from illegal drugs to stolen passwords and data."[27] As explained in another publication,

> An increasing number of cyber criminals are using the dark web — the encrypted part of the internet that cannot be tracked — to shop for software that helps them remain anonymous while carrying out their crimes. The dark web is a part of the deep web, the non-indexed part of the world wide web that cannot be accessed by standard search engines such as Google and requires encrypted networks such as Tor browser.
>
> The most significant feature of this world is that the identity of its users is hidden and cannot be tracked, which is why several illicit products such as weapons and drugs are available here. Cyber criminals, too, appear to be shopping here.[28]

In recent years, technology firms have developed software tools to safely conduct research on the dark web.[29] Using these tools, various databases, and information such as a cybercriminal's moniker, pseudonym, name, email address, or cryptocurrency wallet, technology firms suggest they are able to "connect the dots and unmask bad actors around the globe."[30] While these

[26] N.Y.C. Bar Ass'n, Formal Op. 2010-02 (2010).

[27] Daniel Schiappa, *The Big Business of Cybercrime: The Dark Web*, Forbes Technology Council, FORBES (Sept. 12, 2019), available at https://www.forbes.com/sites/forbestechcouncil/2019/09/12/the-big-business-of-cybercrime-the-dark-web/#d94ff0a5142e (last visited Nov. 20, 2019).

[28] Tushar Kaushik, *Cyber criminals hide in the 'dark web' to remain anonymous*, THE ECONOMIC TIMES (May 2, 2019), available at https://economictimes.indiatimes.com/tech/internet/cyber-criminals-hide-in-the-dark-web-to-remain-anonymous/articleshow/69139795.cms?from=mdr (last visited Nov. 20, 2019).

[29] An example of such a provider is Silo by Authentic8. *See* https://www.authentic8.com/ (last visited Nov. 20, 2019).

[30] *See* 4iQ, available at https://4iq.com/ (last visited Nov. 20, 2019) ("4iQ continuously collects exposed identity information found in open sources on the surface, social, deep, and dark web. More than 14 Billion records found to date are curated into one of the largest collections of compromised identities . . . in order to protect consumers from identity theft and investigate fraud, financial crimes and other threats."); *see id* at https://4iq.com/products/idhunt/ (last visited Nov. 20, 2019) ("Working on behalf of a large US-based financial institution, 4iQ identified a marketplace on the dark web where its customers' login credentials were being sold. Within days, we determined the name, phone number, and hometown of the ringleader, and provided the information — including photographs of the individual —

technologies have been useful in gathering intelligence that can help inform preventative controls and deter fraud, they potentially can be used to trace stolen funds and recover fraudulent transfers.

IV. THIRD-PARTY RECOVERY

A. Common Cybercrime Schemes Involving Fraudulent Electronic Funds Transfers

There are two main cybercrime schemes involving fraudulent funds transfers—Business Email Compromise ("BEC") and Account Takeover. As defined by the FBI's Internet Crime Report, "BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds."[31] In 2018, there were 20,373 incidents of BEC with losses of $1.3 billion.[32] According to an alert issued by the FBI's Internet Crime Complaint Center (IC3) in September 2019,

> The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses. The increase is also due in part to greater awareness of the scam, which encourages reporting to the IC3 and international and financial partners. The scam has been reported in all 50 states and 177 countries. Fraudulent transfers have been sent to at least 140 countries.
>
> Based on the financial data, banks located in China and Hong Kong remain the primary destinations of fraudulent funds. However, the Federal Bureau of Investigation has seen an increase of fraudulent transfers sent to the United Kingdom, Mexico, and Turkey.[33]

The alert further reported that between June 2016 and July 2019, there were 166,349 domestic and international incidents of BEC, with an exposed dollar loss of over $26 billion.[34] For the period

to international authorities. The cost savings have already exceeded more than $100 million from identifying fraudulent credit cards."). Another example is Recorded Future, *see* https://www.recordedfuture.com/solutions/dark-web-monitoring/ (last visited Nov. 20, 2019).

[31] FBI, 2018 *Internet Crime Report*, at 25.

[32] *Id*. at 19-20.

[33] FBI, Internet Crime Complaint Center, Alert No. I-091019-PSA (Sept. 10, 2019) (internal footnote omitted).

[34] *Id*.

between October 2013 and July 2019, there were 69,384 U.S. victims, with an exposed dollar loss of over $10 billion, and 3,624 non-U.S. victims, and with exposed loss of over $1 billion.[35]

The FBI's IC3 defines "Account Takeover" as simply "when a perpetrator obtains account information to perpetrate fraud on existing accounts."[36] More broadly, Account Takeover is described as follows:

> Cybercriminals are . . . using sophisticated methods to obtain access to accounts, including the use of malware (malicious software), SQL injection attacks (SQLIA), spyware, Trojans, and worms. These attacks aim to deliberately exploit a customer's account and, in many instances, to gain seemingly legitimate access to another customer's account. Through ongoing monitoring, financial institutions may identify inconsistencies with a customer's normal account activity that indicates illicit intrusions into a customer's account. Such irregularities might include, but are not limited to, unusual ATM activity, clustered Automated Clearing House (ACH) transactions in different geographic areas, sudden wire transfers, or changes to customer and account profiles.
>
> Account takeover activity differs from other forms of computer intrusion, as the customer, rather than the financial institution maintaining the account, is the primary target. . . . In an account takeover, at least one of the targets is a customer holding an account at the financial institution and the ultimate goal is to remove, steal, procure or otherwise affect funds of the targeted customer.[37]

In 2018, there were 16,128 incidents of Account Takeover (including Identity Theft) with losses of over $100 million.[38]

[35] *Id*.

[36] FBI, *2018 Internet Crime Report*, at 26.

[37] Department of the Treasury, Financial Crimes Enforcement Network, Advisory FIN-2011-A016 (Dec. 19, 2011).

[38] FBI, *2018 Internet Crime Report*, at 19-20.

B. Legal Framework Allocating Commercial Account Losses Due to Cybercrime from Fraudulent Electronic Funds Transfers

The legal framework applied today to cybercrime dates to the 1980s—before online Internet and mobile banking was ever contemplated. That decade marked a shift in banking to electronic funds transfers ("EFTs"), the advent of the personal computer and Internet, and the drafting of Article 4A of the Uniform Commercial Code ("UCC") to address EFTs. By then, the monetary volume of wires and other electronic transfers, over a trillion dollars a day, far exceeded payments by other means.[39] Unlike checks, governed for decades by the Negotiable Instruments Law and then Articles 3 and 4 of the original 1962 UCC, there was no comprehensive body of law that defined the rights and obligations that arose from electronic transfers. In 1989, Article 4A was proposed by the National Conference of Commissioners on Uniform State Law to provide that body of law.

The drafters of Article 4A recognized that an electronic transfer is "not comparable to payment of a check by the drawee bank on the basis of" a forged signature, or altered or counterfeit paper, and thus new rules were required.[40] Rather, "the receiving bank relies on a security procedure pursuant to which the authenticity of the [EFT] message can be 'tested' by various devices . . . designed to provide certainty that the message is that of the sender identified in the payment order."[41] Because EFTs typically are in large amounts, often multimillion dollar "wholesale wire transfers," completed the same day, between sophisticated business or financial organizations, and intended to be efficient, low-cost substitutes for paper instruments, Article 4A

[39] UCC Art. 4A, prefatory note.

[40] UCC § 4A-203, cmt. 1.

[41] *Id.*

was drafted with those defining characteristics in mind, and established governing principles and rules intended to provide for concomitant efficient, low-cost allocation of risk of loss.[42]

Commercial bank customers utilize two primary types of EFTs: traditional wire transfers and Automated Clearing House ("ACH") transactions. Most wire transfers in the United States are conducted via Fedwire, a system operated by the Federal Reserve Banks.[43] The ACH network, an electronic counterpart to the check system, "is a batch processing system in which financial institutions accumulate ACH transactions throughout the day for later batch processing . . . . Settlement, or the transfer of funds from one financial institution to another to complete the transaction, generally happens next day."[44] Businesses typically use the ACH network to make payroll and vendor payments.

Wire transfers and commercial ACH transactions are governed primarily by Article 4A of the revised 1990 UCC, as adopted by the states.[45] In contrast, consumer ACH transactions are governed by the Electronic Funds Transfer Act of 1978 ("EFTA"),[46] generally providing a limit of $50 on the loss that can be allocated to an account holder for any "unauthorized electronic fund

[42] *Id.*

[43] The volume of the Fedwire system is about $2.9 trillion per day, *see* Board of Governors of the Federal Reserve System, *Fedwire Funds Service—Annual*, available at https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm (last visited Oct. 21, 2019), while the private sector Clearing House Interbank Payments System (CHIPS) is about $1.5 trillion per day, *see* The Clearing House, *About CHIPS*, available at https://www.theclearinghouse.org/payment-systems/chips (last visited Oct. 21, 2019).

[44] Nacha, *What is ACH?: Qucik Facts About the Automated Clearing House (ACH) Network*, Oct. 1, 2015, available at https://www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network (last visited Oct. 21, 2019). In 2018, the ACH Network processed about 23 billion payments, representing over $51.2 trillion. Nacha, ACH Network Volume Statistics, https://www.nacha.org/content/what-is-ach (last visited Oct. 21, 2019).

[45] Wire transfers conducted over the FedWire system are subject to Federal Reserve Regulation J, which incorporates UCC Article 4A. *See* 12 C.F.R. § 210.25(b)(1); Utility Supply Co. v. AVB Bank, 2010 U.S. Dist. LEXIS 126948, *9-14 (N.D. Okla. Nov. 30, 2010) (wire transfers conducted over FedWire are governed by Regulation J, incorporating UCC Article 4A as Appendix B to 12 C.F.R. part 210, thereby presenting a federal question). By 1996, Article 4A was adopted by all states and the District of Columbia. Benjamin Geva, THE LAW OF ELECTRONIC FUNDS, § 1.05[2] (Dec. 2009). ACH transactions are also subject to the Operating Rules of the National Automated Clearing House Association ("Nacha").

[46] UCC § 4A-108 ("This Article does not apply to a funds transfer any part of which is governed by the [EFTA]"). The EFTA applies to transfers of funds involving accounts "established primarily for personal, family, or household purposes." 15 U.S.C. § 1693a(2). The EFTA does not apply to wire transfers, such as via Fedwire. Wright v. Citizen's Bank of E. Tenn., 640 Fed. Appx. 401, 404 (6th Cir. 2016).

transfers."[47] As explained in *Patco Constr. Co., Inc. v. People's United Bank,*[48] "consumer payments that are made electronically, such as through direct wiring or the use of a debit card, are covered by a separate federal statute, the Electronic Fund Transfer Act (EFTA). . . . Article 4A does not apply to funds transfers covered by the EFTA; the two are mutually exclusive."[49]

1. UCC Article 4A's General Rules for Allocating Losses

Generally, UCC § 4A-204 imposes liability on a receiving bank[50] for unauthorized transfers by requiring the bank to refund any funds (plus interest) from a payment order[51] that was neither: (1) authorized by the customer under UCC § 4A-202, nor (2) enforceable against the customer under UCC § 4A-203, as not effected by (a) an authorized employee or (b) a person who obtained access to its transmitting facilities, or otherwise obtained transmittal information from the customer. Thus, whether the risk of loss for an unauthorized EFT falls upon the bank or the customer is governed by UCC §§ 4A-202 and 203.

Under subsection 4A-202(a), a payment order is authorized if the person identified as the sender authorized the order or is otherwise bound under the law of agency. Subsection 4A-202(b) further permits the receiving bank to escape liability, even though the customer did not authorize the payment order, if the bank proves: (1) the bank and customer agreed that the authenticity of a payment order would be verified through a "security procedure;" (2) the security procedure agreed upon is "commercially reasonable;" (3) the bank processed the payment order in "compliance" with the security procedure; (4) the bank processed the order in compliance with any written

[47] 15 U.S.C. § 1693g.

[48] 684 F.3d 197 (1st Cir. 2012).

[49] *Id*. at 207 n.7. *See* Binns v. BB&T Bank, 2019 U.S. Dist. LEXIS 76113, *9-10 (E.D. Pa. May 6, 2019) (applying same).

[50] A "receiving bank" is the bank receiving the payment order, typically, the customer's bank. UCC § 4A-103(a)(4).

[51] A "payment order" is the instruction to the receiving bank to pay a fixed or determinable amount of money. UCC § 4A-103(a)(1).

agreement or instruction of the customer; and (5) the bank accepted the payment order in "good faith."[52]

Unless all five elements are met, the receiving bank will be strictly liable for any unauthorized EFT.[53] Even if these conditions are satisfied, the risk of loss will still shift to the bank if "the person committing the fraud did not obtain the confidential information [facilitating breach of the security procedure] from an agent or former agent of the customer or from a source controlled by the customer. . . ."[54]

As will be shown below, in evaluating whether a receiving bank or its customer should bear the loss for a fraudulent EFT, the key determination is whether the bank's security procedures were commercially reasonable under the UCC and developing case law. This determination focuses on: (a) the terms of the bank-customer agreement; (b) whether the security procedures complied with banking agency guidelines; (c) whether the security procedures were designed to meet the circumstances of the customer, as opposed to a one-size-fits-all approach; and (d) whether the bank implemented and followed commonly available security procedures in connection with the transactions at issue.

2. Agreed Verification "Security Procedure"

A "security procedure" is a "procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order . . . is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication."[55]

[52] UCC § 4A-202(b).
[53] UCC § 4A-204(a).
[54] UCC § 4A-203 cmt. 5.
[55] UCC § 4A-201.

A "security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices."[56]

In *Experi-Metal, Inc. v. Comerica Bank*,[57] the agreed security procedure required the customer to input its user identification, four-digit PIN, and a six-digit code from a secure token (a randomly generated number that changed every 60 seconds).[58] In an effort to avoid liability under UCC § 4A-202(c), discussed *infra*, for not complying with the agreed procedure, the bank contended it offered the customer the ability to require two individuals to approve wire transfers as an additional security procedure, which the customer refused.[59] The U.S. District Court for the Eastern District of Michigan rejected the argument, noting that "requiring confirmation by additional users simply is an option or element within a security procedure. The 'security procedure' is the secure token technology" which the court found by itself commercially reasonable,[60] as discussed further *infra*.

A "security procedure" does not include "procedures that the receiving bank may follow unilaterally in processing payment orders,"[61] such as its internal policies and procedures. Thus, a bank cannot point to internal procedures not contained in the customer agreement to bolster its "security procedure" as being "commercially reasonable." In *Chavez v. Mercantil Commercebank, N.A.*,[62] the U.S. Court of Appeals for the Eleventh Circuit rejected the bank's reliance on a catch-all clause in its customer agreement that it "may use . . . any other means to verify any Payment Order or related instruction" to show additional internal procedures were part of its "security procedures," where the agreement provided a specific security procedure.

[56] *Id*.

[57] 2010 U.S. Dist. LEXIS 68149 (E.D. Mich. July 8, 2010).

[58] *Id*. at *11-14.

[59] *Id*. at *11-14.

[60] *Id*. at *14.

[61] UCC § 4A-201 cmt.

[62] 701 F.3d 896, 901-04 (11th Cir. 2012).

Similarly, a bank's internal fraud procedures not incorporated in the customer agreement, such as verifying new payees, applying daily or item limits, or fraud profile screening would not be relevant to whether there was "compliance" with the "security procedure" in processing a wire or ACH transfer. By the same token, a bank's failure to follow its internal procedure for processing EFTs should be not be considered a failure to follow an agreed "security procedure."[63]

A specific "security procedure" need not be identified in the customer agreement if it simply provides that the bank will select security procedures that are commercially reasonable, according to the U.S. District Court for the Southern District of New York in *Brago Filho v. Interaudi Bank*,[64] which reasoned:

> By signing the [customer agreement] plaintiffs agreed to the Bank's security procedures, so long as they are found to be commercially reasonable. It does not matter that plaintiffs did not know what the Bank's security procedures were because [UCC Article 4A] compels banks to use commercially reasonable procedures. Indeed, a bank that chooses unreasonable procedures does so at its peril.[65]

In *Choice Escrow and Land Title, LLC v. BankcorpSouth Bank*,[66] the customer declined "Dual Control," as offered by the bank, requiring two user, separate logins and passwords to process wire transfers, and daily limits on wire activity. When the customer later inquired whether foreign wire transfers could be blocked to avoid fraud, the bank advised it was unable to stop foreign wires only, re-offering dual control which the customer again refused. After a loss, the customer argued the security procedures offered were not commercially reasonable where none involved transactional analysis subjecting wires to individual fraud review. The Eighth Circuit,

[63] *See* Skyline Int'l Development v. Citibank, F.S.B., 706 N.E.2d 942, 945 (Ill. App. 1998) (bank's admitted failure to follow internal procedure for obtaining wire transfer authorization not relevant to whether bank followed agreed "security procedure").

[64] 2008 U.S. Dist. LEXIS 31443 (S.D.N.Y. Apr. 16, 2008).

[65] *Id*. at *15.

[66] 754 F.3d 611 (8th Cir. 2014).

affirming the district court, held it was impracticable for the bank to review every outgoing wire, and that there was no genuine issue of fact whether reasonable commercial procedures required the use of transactional analysis. The court further held the security procedures offered were commercially reasonable for the customer, observing:

> [T]his appears to be a case where "an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper[,]" in which case "the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank."[67]

In *Envision Healthcare, Inc. v. FDIC*,[68] the court held the bank not liable for an unauthorized wire transfer resulting from stolen online credentials where it complied with the customer's agreed security procedure: "If an online order were placed with a valid password, the bank promised it would verify the validity of the password, no more, and the parties agreed the bank would not be liable for any transaction (authorized or not) conducted while using that password."[69]

In *Banco del Austro, S.A. v. Wells Fargo Bank, N.A.*,[70] Wells Fargo argued that Banco Del Austro agreed (1) funds transfers would be verified by SWIFT (Society for Worldwide Interbank Financial Telecommunication) authentication procedures, and (2) the security procedure was commercially reasonable.[71] The applicable Wells Fargo correspondent banking agreement provided:

[67] *Id*. at 627 (quoting UCC § 4A-203 *cmt*. 4).
[68] 2014 U.S. Dist. LEXIS 167570 (N.D. Ill. Dec. 3, 2014).
[69] *Id*. at *18. The court briefly referenced the "commercially reasonable" requirement of UCC § 4A-202, *id*. at *26, without making a determination.
[70] 215 F. Supp. 3d 302 (S.D.N.Y. 2016).
[71] Def. Wells Fargo Bank, N.A.'s Mem. in Supp. of Mot. to Dismiss, Doc. No. 15, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Feb. 18, 2016), at 9. Several other cases of fraudulent transfers involving SWIFT have been reported. Tom Bergin and Nathan Layne, *Special Report, Cyber thieves exploit bank's faith in SWIFT transfer network*, REUTERS, May 20, 2016, available at https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD (last visited Oct. 23, 2019).

> All payment orders or amendments and cancellations thereof must be transmitted to Wells Fargo in compliance with Security Procedures. . . . The following Security Procedures will be used to verify that Correspondent is the originator of a payment order, or is the sender of other communication requesting an amendment, cancellation or other action regarding a payment order for the communications systems listed below.
>
> For SWIFT, the SWIFT Authentication procedures in accordance with the SWIFT User Handbook as amended from time to time. . . . Correspondent agrees that the above described Security Procedures are commercially reasonable in light of Correspondent's circumstances and the type, value and frequency of the payment orders Correspondent will request.[72]

Banco del Austro did "not allege that Wells Fargo failed to adhere to SWIFT authentication procedures,"[73] but that the agreed security procedure included required fraud detection policies and procedures. Banco Del Austro pointed to the provision in the agreement that "Wells Fargo is a bank organized and existing under the Laws of the US, and intends to comply with all Laws of the US . . . , including without limitation the USA PATRIOT Act, . . . [and] regulations of the United States Department of the Treasury."[74] It cited Treasury Department regulations under the Bank Secrecy Act for correspondent accounts as requiring policies and procedures to detect money laundering activity.[75] It further cited a July 31, 2014 Wells Fargo letter stating its Global Financial Crimes Management Program included: "identifying unusual activity; automated transaction monitoring; customer surveillance; investigating the unusual activities identified, and determining whether they are suspicious; monitoring customer activity, and apply predictive analysis for customer-centric, cross-channel fraud detection; screening, blocking, and rejecting transactions appropriately; and reporting these matters . . . ."[76]

[72] Wells Fargo Bank, N.A., *Terms & Conditions for Global Financial Institutions*, at 4.
[73] Banco del Austro, S.A. v. Wells Fargo Bank, N.A., 215 F. Supp. 3d 302, 304 (S.D.N.Y. 2016).
[74] *Id*. at 304; Wells Fargo Bank, N.A., *Terms & Conditions for Global Financial Institutions*, at 14.
[75] Pl. Banco del Austro, S.A.'s Mem. of Law in Opp. to Def. Wells Fargo Bank, N.A.'s Mot. to Dismiss, Doc. No. 21, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Mar. 31, 2016), at 19-20.
[76] *Id*. at 20.

> The court rejected Banco del Austro's argument, finding the agreement

> requires only that Wells Fargo adhere to the SWIFT authentication procedures when processing orders received via SWIFT. The provision on which Banco del Austro relies did not transform any and all violations of federal and state law into breaches of contract and did not modify the security procedure explicitly outlined under separate header. Thus, Banco del Austro has failed sufficiently to allege that Wells Fargo did not accept the request for the Transfers in compliance with the agreed-upon security procedure.[77]

3. Commercially Reasonable Security Procedures

a. Legal Standards. The UCC's drafters recognized that a principal issue likely to arise in litigation involving fraudulent EFTs is whether any security procedure was commercially reasonable.[78] To promote uniformity the drafters in Article 4A, unlike Articles 3 and 4, provided that the issue of "commercial reasonableness of a security procedure is a question of law."[79] As explained in the Article 4A Official Comments ("Comments"): "It is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers."[80] Whether the bank complied with any security procedure remains a question of fact.[81]

A court may find commercial reasonableness in one of two ways. Under the first method, a "security procedure" is deemed reasonable if:

> (i) 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 (ii) the customer expressly agreed in writing to be bound by any

[77] *Banco del Austro,* 215 F. Supp. 3d at 304.

[78] UCC § 4A-203 cmt. 4.

[79] UCC § 4A-202(c); *cf.* UCC § 3-103(a)(9) (reasonable commercial standards applicable to claims under UCC Articles 3 and 4).

[80] UCC § 4A-203 cmt. 4. *See* Essgeekay Corp. v. TD Bank, N.A., 2018 U.S. Dist. LEXIS 214691, *6-10 (D.N.J. Dec. 19, 2018) (determining as matter of law on motion to dismiss that security procedures involving two-factor authentication were commercially reasonable).

[81] UCC § 4A-203 cmt. 4.

> 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.[82]

The focus in this provision is on the content of the customer agreement. If

> an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper[,] . . . the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank. But this result follows only if the customer expressly agrees in writing to assume that risk.[83]

In cases where a customer rejects security measures offered by the bank, the customer will bear the risk of loss, and be unable to complain that the bank acted "in bad faith by so doing so long as the customer is made aware of the risk."[84]

In the event "a commercially reasonable security procedure is not made available to the customer, subsection [4A-202](b) does not apply. . . . The bank acts at its peril in accepting a payment order that may be unauthorized."[85] Article 4A recognizes that prudent banking practices require that security procedures should be utilized for all EFTs, and 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."[86]

The second method is more complex. Whether a security procedure is commercially reasonable is determined by considering primarily four factors:

(1) "the wishes of the customer expressed to the bank;"

(2) "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;"

[82] UCC § 4A-202(c).
[83] UCC § 4A-203 cmt. 4.
[84] UCC § 4A-203 cmt. 4.
[85] UCC § 4A-203 cmt. 3.
[86] *Id*.

(3) "alternative security procedures offered to the customer;" and

(4) "security procedures in general use by customers and receiving banks similarly situated."[87]

Applying these factors is not a simple task. According to the Comments, "the concept of what is commercially reasonable in a given case is flexible," a pronouncement at odds with Article 4A's policy goal of creating a uniform standard by having the issue decided as a matter of law.[88] The Comments also contain other conflicting guidance:

> The purpose of subsection (b) is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The 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, which is a lower standard. On the other hand, a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable.[89]

In addition, the Comments introduce other factors. The first is a cost-benefit analysis:

> Verification entails labor and equipment costs that can vary greatly depending upon the degree of security that is sought. A customer that transmits very large numbers of payment orders in very large amounts may desire and may reasonably expect to be provided with state-of-the-art procedures that provide maximum security. But the expense involved may make use of a state-of-the-art procedure infeasible for a customer that normally transmits payment orders infrequently or in relatively low amounts.[90]

The second "is the type of receiving bank. It is reasonable to require large money-center banks to make available state-of-the-art security procedures. On the other hand, the same requirement may not be reasonable for a small country bank."[91] A third is that the bank may offer different security

[87] UCC § 4A-202(c).
[88] UCC § 4A-203 cmt. 4.
[89] *Id.*
[90] *Id.*
[91] *Id.*

procedures to different customers: "A receiving bank might have several security procedures that are designed to meet the varying needs of different customers."[92]

In *Patco*, *supra*,[93] the U.S. Court of Appeals for the First Circuit, reversing a Maine district court,[94] held the bank's security procedures were not commercially reasonable. There a customer's computer infected by the Zeus/Zbot malware allowed cybercriminals to steal Patco's login credentials and withdraw $588,851 in a series of large ACH transfers over several days in May 2009.[95] Patco used online banking to make ACH transfers for weekly payroll involving recurrent characteristics: they were always made on Fridays; initiated from computers in its Maine office; originated from a single static Internet Protocol ("IP") address; accompanied by tax withholdings and 401(k) contributions; and in modest amounts, the largest $36,634.[96] The security procedure utilized by the bank consisted of: (1) user IDs and passwords; (2) invisible device authentication, which placed "device cookies" to identify computers used to access online banking; (3) risk profiling, creating a profile for each customer based on its online banking usage to compare transaction; and (4) challenge questions and answers based on a dollar threshold for certain transactions.[97] The bank originally set the challenge question procedure to transactions over $100,000 for all customers, and subsequently lowered the threshold to $1.[98] As the First Circuit noted, "[t]here were several additional security measures that were available to [the bank] that [it] chose not to implement," including: (1) Out-of-Band Authentication, such as notification to the customer via telephone or other means; (2) User-Selected Picture; (3) Password-Generating

[92] *Id.*
[93] 684 F.3d 197 (1st Cir. 2012).
[94] 2011 U.S. Dist. LEXIS 58112 (D. Me. May 27, 2011), *adopted by*, 2011 U.S. Dist. LEXIS 86169 (D. Me. Aug. 4, 2011).
[95] 684 F.3d at 204-06.
[96] *Id.* at 200.
[97] *Id*. at 202-03.
[98] *Id*. at 203.

Security Tokens; and (4) Monitoring of Risk-Scoring Reports (the latter two of which the bank adopted after the fraud).[99] The fraudulent withdrawals were directed to new payees, originated from computers not recognized by the bank, and from an IP address Patco never used, resulting in high-risk scores of 790, 785, 720 and 563, a "significant departure" from Patco's usual scores of 10 to 214, but the bank had no procedure in place to monitor high-risk scores or to notify the customer.[100]

The First Circuit concluded that the bank's collective failures rendered its security procedures commercially unreasonable:

> In our view, Ocean Bank did substantially increase the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and high dollar transfers [because frequent answers were more exposed to capture by malware]. Then, when it had warning that such fraud was likely occurring in a given transaction, Ocean Bank neither monitored the transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable.[101]

The court emphasized that the bank's adoption of a "one-size-fits-all" $1 threshold for all customers, to target universally low-dollar fraud, violated "Article 4A's instruction to take the customer's circumstances into account."[102] It also based its conclusion on the fact that the bank did not utilize other security measures "not uncommon" in the industry, including manual reviews of high-risk transactions and the use of password-generating security tokens.[103]

In *Essgeekay Corp. v. TD Bank, N.A.,*[104] the court held on motion to dismiss a bank's security procedures commercially reasonable as a matter of law because they contained two-factor

[99] *Id*. at 203-04.
[100] *Id*. at 204-05.
[101] *Id*. at 211.
[102] *Id*. at 212.
[103] *Id*. at 212-13.
[104] 2018 U.S. Dist. LEXIS 214691, *6-10 (D.N.J. Dec. 19, 2018).

authentication procedures in accord with banking agency guidelines. Specifically, the procedures consisted of (1) login information and security questions – "something the user knows" – and (2) unfamiliar device lockout – "something the user has."[105]

Two other cases focus on the content of bank-customer agreements in finding the bank's security procedures to be commercially reasonable. In *Experi-Metal,*[106] the district court confined its analysis to the "plain and unambiguous terms" of the deposit agreement, finding the bank's "secure token technology was reasonable" merely because the customer agreed to it in its contract with the bank.[107] The court rejected as parole evidence the customer's expert opinion that secure token technology was not a commercially reasonable security procedure.[108] In *All American Siding & Windows, Inc. v. Bank of America, N.A.*,[109] a Texas court similarly relied on online banking agreements in which the customer "agreed that the authenticity of ACH transactions were to be verified using an ID, passcode, and digital certificate verification."[110] Based on the agreements and a bank affidavit that it "follow[ed] the guidelines of the Federal Financial Institution Examination Counsel and requires multifactor authentication for its online banking customers," the court held the security procedures commercially reasonable, entitling the bank to summary judgment.[111]

b. Banking Regulatory Agency Guidelines. As recognized by the First Circuit in *Patco* and other courts, the guidelines issued by the Federal Financial Institutions Examination

[105] *Id*. at *10.

[106] 2010 U.S. Dist. LEXIS 68149 at *16-17.

[107] *See also* Transamerica Logistic, Inc. v. JPMorgan Chase Bank, N.A., 2008 U.S. Dist. LEXIS 112708, at *3 & n.1 (S.D. Tex. July 21, 2008) (agreement contained stipulation that customer "acknowledge[d] and agree[d] that the security procedures described [in the agreement] are commercially reasonable" and customer did not offer "contradictory evidence or argument").

[108] *Id.*

[109] 367 S.W.3d 490 (Tex. App. 2012).

[110] *Id*. at 500-501.

[111] *Id*. at 500-502.

Council ("FFIEC") establish relevant guideposts for evaluating whether bank security procedures are commercially reasonable.[112] To begin with, financial institutions are required to have a comprehensive written information-security program. Among other mandates, the security program must be designed to "protect against unauthorized access to or use of [customer] information that could result in substantial harm or inconvenience to any customer."[113] These guidelines further require:

> an institution's information security program be monitored, evaluated, and adjusted as appropriate in light of changes in technology, the sensitivity of customer information, internal and external threats to information, the institution's changing business arrangements, and changes to customer information systems. These same criteria apply to re-evaluating the institution's Internet banking controls.[114]

FFIEC, and the federal banking agencies in turn, issued specific guidance to banks for adopting security measures to avoid fraudulent EFTs in its October 2005 publication, *Authentication in an Internet Banking Environment* (the "FFIEC 2005 Guidelines").[115] At that time, the agencies "consider[ed] single factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties,"[116] noting "[a]ccount fraud and identity theft are frequently the result of single-factor (*e.g.*, ID/password) authentication exploitation."[117] Thus, "financial institutions should implement multifactor authentication, layered security, or other controls . . . in light of new

[112] 684 F.3d at 201-04.

[113] FFIEC, I*nteragency Guidelines Establishing Information Security Standards* (Mar. 29, 2005), at Sec. II, B. 3 (codified at 12 C.F.R. pt. 364, App. B (FDIC)); *see also* FFIEC, *Interagency Guidelines Establishing Information Security, Small-Entity Compliance Guide* (Dec. 14, 2005); FFIEC, *Information Security, IT Examination Handbook* (Sept. 2016).

[114] FFIEC, *Frequently Asked Questions on FFIEC Authentication in an Internet Banking Environment*, at 5 (Aug. 15, 2006).

[115] FFIEC, *Authentication in an Internet Banking Environment* (Oct. 12, 2005).

[116] *Id*. at 1.

[117] *Id*.

or changing risks, such as phishing, pharming, malware, and the evolving sophistication of compromise techniques."[118]

The FFIEC 2005 Guidelines outlined control features that banks may employ as part of a multifactor authentication strategy. The first is "out-of-band" authentication which includes "any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction."[119] Examples of "out-of-band" procedures include callback verification to the same or another person at the customer, email approval or notification, or text message-based challenge/response processes.[120] A second category involves verification of internet protocol address ("IPA") location and geo-location.[121] Each computer on the Internet is assigned an IPA. When a customer accesses the bank's site, a profile is created identifying the IPA used. If a new IPA is identified that does not match the customer's IPA profile, access to the bank's site will be denied. Geo-location is another technique to limit Internet users by determining where they are located to identify whether the distance is considered reasonable in relation to the bank.[122] A third category is mutual authentication, whereby "customer identity is authenticated and the [bank's web] site is authenticated to the customer."[123] One method is "[t]he use of digital certificates coupled with encrypted communication (e.g. Secure Socket Layer, or SSL) . . . ."[124]

Finally, the FFIEC 2005 Guidelines advised: "Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. Much of this control is not based directly upon authentication. For example, a financial institution can analyze the activities

[118] *Id*. at 4 (footnotes omitted).
[119] *Id*. at 11.
[120] *Id*. at 3, n.5, 11-12.
[121] *Id*. at 12.
[122] *Id*. at 12-13.
[123] *Id*. at 13.
[124] *Id*.

of its customers to identify suspicious patterns,"[125] a common fraud detection technique long used by banks. "Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit,"[126] another longstanding technique.

In June 2011, FFIEC issued a *Supplement to Authentication in an Internet Banking Environment* ("FFIEC 2011 Supplement"), recommending that banks use a layered security framework, covering five core areas: (1) fraud detection and monitoring; (2) multifactor authentication; (3) Internet protocol and device analysis; (4) transaction limits and controls; and (5) customer education.[127] FFIEC observed that "manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior."[128] Therefore, as part of a bank's layered security program, the following two elements are now mandated. First, a bank's program must have "processes to detect anomalies and effectively respond to suspicious or anomalous activity related to:" (a) customer login and authentication; and (b) online funds transfers.[129] Second, the program should include enhanced controls for customer administrators who have authority to set up or change system

[125] *Id*. at 5. Separately, the Bank Secrecy Act ("BSA") requires banks to have BSA/anti-money laundering compliance programs and appropriate policies, procedures, and processes in place to monitor account activity and identify unusual activity, such as transactions inconsistent with the nature of the customer's business, or any other suspicious activity. *See generally*, FFIEC, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2014; updated May 5, 2018). FFIEC views electronic banking as a "potentially higher-risk area" of banking, requiring commensurate anti-fraud policies, procedures, and processes. *See id.* at 202-26 (addressing electronic banking, funds transfers, and ACH transactions). The federal banking agencies have also implemented Identity Theft Red Flags Rules and Guidelines, requiring banks to have policies and procedures to identify patterns, practices, or activities that indicate possible identity theft. These rules apply to consumer accounts and other accounts for which there is a foreseeable risk of identity theft, such as small business and sole proprietorship accounts. *See, e.g.*, 12 C.F.R. § 334.90 (FDIC); 72 Fed. Reg. 63,718, at 63,721 (Nov. 9, 2007); FDIC Press Release, FDIC-PR-88-2009, *Agencies Issues Frequently Asked Questions on Identity Theft Rules* (Jun. 11, 2009).

[126] *Id*.

[127] FFIEC, *Supplemental to Authentication in an Internet Banking Environment* (June 28, 2011), at 3-8.

[128] *Id*. at 5.

[129] *Id*.

configurations.[130] The agencies also point out that "[l]ayered security controls do not have to be complex. For example, implementing time of day restrictions on the customer's authority to execute funds transfers or using restricted funds transfer recipient lists, in addition to robust logon authentication, can help to reduce the possibility of fraud."[131]

Because most banks rely on third-party technology service providers for their Internet banking platform, FFIEC has re-emphasized that banks have ultimate responsibility for such outsourced activities. In October 2012, FFIEC issued two manuals in this area: the *Supervision of Technology Service Providers*, part of its *IT Examination Handbook*; and new *Administrative Guidelines for the Implementation of the Interagency Program for the Supervision of Technology Service Providers*.

In December 2013, FFIEC issued guidelines to address activities conducted by banks via social media. Emphasizing that "[s]ocial media is one of several platforms vulnerable to account takeover and the distribution of malware," FFIEC and the federal banking agencies advise that banks "should ensure that the controls it implements to protect its systems and safeguard customer information from malicious software adequately address social media usage."[132]

In June 2015, FFIEC released a voluntary Cybersecurity Assessment Tool to help banks identify "their risks and determine their cybersecurity preparedness."[133] The Assessment, updated in May 2017, consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile is used to identify a bank's inherent risk based on five categories: Technologies and Connection Types; Delivery Channels; Online/Mobile Products and Technology

[130] *Id*.

[131] *Id*. at 11-12.

[132] FFIEC, *Social Media: Consumer Compliance Risk Management Guidance* (Dec. 11, 2013), at 19.

[133] FFIEC, *FFIEC Releases Cybersecurity Assessment Tool* (June 30, 2015).

Services; Organizational Characteristics; and External Threats.[134] The Cybersecurity Maturity is used to evaluate a bank's maturity level in five domains: Cyber Risk Management and Oversight; Threat Intelligence and Collaboration; Cybersecurity Controls; External Dependency Management; and Cyber Incident Management and Resilience.[135] In August 2019, FFIEC issued a statement that banks should adopt a standardized tool to access and improve cybersecurity preparedness, whether they use FFIEC's Cybersecurity Assessment Tool, or other available tools, including the National Institute of Standards and Technology Cybersecurity Framework, the Financial Services Sector Coordinating Council Cybersecurity Profile, and the Center for Internet Security Critical Security Controls.[136]

In June 2016, FFIEC issued a statement on safeguarding the Cybersecurity of Interbank Messaging and Wholesale Payment Networks to advise banks to actively manage the risks associated with interbank messaging and wholesale payment networks, such as SWIFT.[137]

In September 2016, FFIEC issued a revised Information Security manual, as part of its IT Examination Handbook, providing further guidance on managing information security risks.[138]

In addition to the federal banking agencies, states have become involved in issuing cybersecurity regulations. Most notably, the New York State Department of Financial Services issued Cybersecurity Requirements for Financial Services Companies, effective in March 2017, requiring New York-state chartered banks and other covered entities, among other things, to adopt cybersecurity policies and to file annual certifications of compliance.[139]

[134] FFIEC, *FFIEC Cybersecurity Assessment Tool* (May 2017), at 1.
[135] *Id*.
[136] FFIEC, *FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness* (Aug. 28, 2019).
[137] FFIEC, *Cybersecurity of Interbank Messaging and Wholesale Payment Networks* (Jun. 6, 2016).
[138] FFIEC, *FFIEC Information Technology Examination Handbook, Information Security* (Sept. 2016).
[139] 23 NYCRR pt. 500.

4. "Compliance" With Security Procedures and Written Instructions

The bank must prove it complied with the security procedure in processing a payment order under the third element of UCC subsection 4A-202(b), which provides: "If the fraud was not detected because the bank's employee did not perform the acts required by the security procedure, the bank has not complied."[140]

Similarly under the fourth element, the bank must prove that it complied with "any written agreement or instruction of the customer restricting acceptance of payment orders . . . ."[141] The Comments recognize that a customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank. . . . Such limitations may be incorporated into the security procedure itself or they may be covered by a separate agreement or instruction."[142] The Comments provide several examples of limitations customers may impose:

> [T]he customer may prohibit the bank from accepting a payment order that is not payable from an authorized account, that exceeds the credit balance in specified accounts of the customer, or that exceeds some other amount. Another limitation may relate to the beneficiary. The customer may provide the bank with a list of authorized beneficiaries and prohibit acceptance of any payment order to a beneficiary not appearing on the list.[143]

As discussed, the banking agencies recognize these types of limitations as an appropriate part of a bank's layered security control program.

5. Bank Must Prove It Acted In "Good Faith"

As the fifth and final element, the receiving bank must prove that it processed the payment order in good faith.[144] Under Article 4A, "good faith" is defined as "honesty in fact and the

[140] UCC § 4A-203 cmt. 3.
[141] UCC § 4A-202(b).
[142] UCC § 4A-203 cmt. 3.
[143] *Id.*
[144] UCC § 4A-202(b).

observance of reasonable commercial standards of fair dealing."[145] "Honesty in fact" is measured by a subjective standard, requiring a court to examine the facts surrounding the transaction.[146] The bank's "observance of reasonable commercial standards of fair dealing," however, is evaluated by an objective measure of the fairness of the party's action in light of prevailing commercial standards.[147] "Although 'fair dealing' is a broad term that must be defined in context, it is clear that it is concerned with the fairness of conduct rather than the care with which an act is performed."[148]

In *Choice Escrow*, the Eighth Circuit described the good faith test as follows:

> [W]hile there may be some evidentiary overlap between the commercial reasonableness of a bank's security procedures and its compliance with reasonable commercial standards of fair dealing, we do not believe that the two inquiries are coextensive. While the commercial reasonableness inquiry concerns the adequacy of a bank's security procedures, the objective good faith inquiry concerns a bank's acceptance of payment orders in accordance with those security procedures. In other words, technical compliance with a security procedure is not enough under Article 4A; instead . . . the bank must abide by its procedures in a way that reflects the parties' reasonable expectations as to how those procedures will operate.
>
> [T]he focus of our good faith inquiry is on the aspects of wire transfer that are left to the bank's discretion. . . .Where, as here, a bank's security procedures do not depend on the judgment or discretion of its employees, the scope of the good-faith inquiry under Article 4A is correspondingly narrow. . . . [T]o establish that it acted in good faith, [the bank] must establish that its employees accepted and executed the . . . payment order in a way that comported with [the customer's] reasonable expectations, as established by reasonable commercial standards of fair dealing.[149]

In *Experi-Metal,* having concluded the security procedure was commercially reasonable, the court then addressed the further issue whether the bank handled the wires at issue in good faith. On January 22, 2009, criminals hacked into the customer's account, and between 7:30 a.m. and

[145] UCC § 4A-105(d)(incorporating definitions of Article 1); UCC § 1-201(20).
[146] UCC 1-201 cmt. 20; Maine Family Fed. Credit Union v. Sun Life Assurance Co. of Canada, 727 A.2d 335, 340-42 (Me. 1999).
[147] UCC 1-201 cmt. 20; *Maine Family Fed. Credit Union*, 727 A.2d at 340-42.
[148] UCC § 1-201 cmt. 20.
[149] 754 F.3d at 623.

10:50 a.m., the bank processed 47 wire transfers to accounts in Russia, Estonia, Scotland, Finland, China, and the United States. Between 10:53 a.m. and 2:02 p.m., it processed another 46 wires. Altogether it transferred $1.9 million from the customer's account.[150] In two preceding years, the customer made only two wire transfers, both in 2007.[151] In view of prior wire activity, the number of sudden wires, and their destinations, the court found a genuine issue of fact existed whether the bank acted in good faith.[152] At a bench trial, the court ruled for the customer. The bank presented evidence only on the subjective element of good faith, failing to "present evidence from which this Court could determine what the 'reasonable commercial standards of fair dealing' are for a bank responding to a phishing incident . . . and thus whether" the bank satisfied "the objective prong of the 'good faith' requirement."[153] As a result, the court as "trier of fact [was] inclined to find that a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier."[154]

Banco del Austro,[155] also illustrates the question of good faith. Banco del Austro, S.A., an Ecuadorian bank, maintained a correspondent banking relationship with Wells Fargo Bank, N.A. in New York for conducting international funds transfers. In 2015 Banco del Austro's computer system was infiltrated by cybercriminals who stole the login credentials of a bank employee, logged on to its SWIFT terminal and caused at least 13 unauthorized transfers by re-issuing previously cancelled or rejected transactions in its SWIFT outbox by altering the amounts, beneficiary, beneficiary bank, and destination. Between January 12 and 21, 2015, a dozen SWIFT

[150] 2010 U.S. Dist. LEXIS 68149, *6-9.

[151] *Id*. at *19-20.

[152] *Id*. at *18-19, 21-23 (citing In re Jersey Tractor Trailer Training, Inc., 580 F.3d 147 (3d Cir. 2009) and *Maine Family Fed. Credit Union*, 727 A.2d 335).

[153] Experi-Metal, Inc. v. Comerica Bank, 2011 U.S. Dist. LEXIS 62677, *35 (E.D. Mich. June 13, 2011).

[154] *Id.* at *38.

[155] Banco del Austro, S.A. v. Wells Fargo Bank, N.A., 215 F. Supp. 3d 302 (S.D.N.Y. 2016).

messages were sent from Banco del Austro to Wells Fargo, directing fraudulent transfers totaling $12,172,762. Banco del Austro alleged the transfers were unusual, suspect, or anomalous as inconsistent with its normal activity in its correspondent account at Wells Fargo. Specifically, Banco del Austro alleged the fraudulent transfers were suspicious because:

(1) all were outside normal operating hours of the SWIFT payment orders;

(2) many were in unusual amounts, with 7 over $1 million;

(3) the beneficiaries and geographic locations were unusual, including 9 transfers to Hong Kong;

(4) the frequency was unusual: 12 transfers in nine days, 3 to the same entity in 26 hours;

(5) the same entity in Hong Kong received substantial funds from different customers of Banco del Austro within the 26-hour period.[156]

Given these circumstances, the court ruled that factual matters outside of the complaint were required to determine whether SWIFT's procedures by themselves constituted a commercially reasonable security procedure and whether Wells Fargo acted in good faith:

> The Court cannot now determine the commercial reasonableness of the agreed-upon security procedure or, by extension, whether Wells Fargo complied with reasonable commercial standards of fair dealing when it processed the Transfers pursuant to that procedure. In defining that procedure, the Agreement incorporates wholesale the SWIFT user manual, a document outside of the complaint. Further, both parties in their memoranda urge upon the Court news articles and industry publications detailing the security bonafides and vulnerabilities of the SWIFT system. Resort to these extra-complaint sources illustrates the fact-intensive nature of the commercial reasonableness inquiry, one that courts typically address at summary judgment. At bottom, the facts alleged in the complaint and its exhibits do not permit the Court to rule as a matter of law that use of the SWIFT system, with nothing more, constituted a commercially reasonable security procedure in the context of this particular customer-bank relationship.[157]

[156] Complaint, Doc. No. 1-1, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Jan. 28, 2016), at 5–9.

[157] *Banco Del Austro,* 215 F. Supp. 3d at 306 (citations omitted).

The court denied Well Fargo's motion to dismiss the claims under UCC Article 4A,[158] and shortly thereafter the case settled.[159]

In *Essgeekay Corp.*, the court denied the bank's motion to dismiss on the grounds that the customer "sufficiently pleaded that [the bank] failed to accept the payment orders in good faith and in compliance with the security procedure." *Id.* at *13. The customer alleged that on previous occasions the bank's security procedures blocked access to the account when an unfamiliar device was used, forming "the foundation upon which Plaintiff's expectations rest." *Id.* at *12. The customer also alleged that the bank "ultimately locked" the account because it "*suspected* that the activity was fraudulent." *Id.* at *13 (emphasis in original). Recognizing that good faith is a "question of fact," *id.* at *11, the court concluded:

> Thus, taking the Complaint's factual allegations as true and drawing all reasonable inferences in favor of Plaintiff, as the Court must do, the inference can be drawn that [the bank] failed to prevent an unauthorized individual from accessing the account on an unknown computer, and that [the bank] permitted these transfers to go through *despite* being unable to confirm their authenticity with [the customer] and *despite* suspicions that they were fraudulent.

Id. at *13 (emphasis in original). That case too settled shortly thereafter.

In *Patco*, after finding the bank's security procedure to be commercially unreasonable, the First Circuit affirmed the denial of Patco's cross-motion for summary judgment and remanded the case. Raising an issue not reached or briefed below, the appeals court noted "[i]t is unclear . . . what, if any, obligations a commercial customer has when a bank's security system is found to be

[158] *Id.*

[159] After the parties conducted discovery, Wells Fargo moved for summary judgment, filing under seal. Def. Wells Fargo Bank, N.A.'s Mem. of Law in Supp. of Mot. for Summary Judgment, Doc. No. 48, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Oct. 3, 2017). Before Banco del Austro filed its opposition, the court denied the motion without prejudice. Order, Doc. 54, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Oct. 18, 2017). Illustrating the fact-intensive nature of the dispute, the court reasoned that Wells Fargo could raise the same arguments at a bench trial, the parties having waived trial by jury. *Id.*

commercially unreasonable."[160] While seemingly broad, the issue as framed by the First Circuit narrowly addressed the remaining loss-allocation rule of Article 4A, section 4A-204.[161] That section provides, *inter alia*, that where no commercially reasonable security procedure is in effect, the bank shall refund any unauthorized payments, and further, pay interest unless "the customer fails to exercise ordinary care to determine that the order was not authorized . . . and to notify the bank . . . within a reasonable period of time not exceeding 90 days . . . ."[162] This customer obligation of ordinary care pertains only to whether it may recover interest, otherwise "the bank takes the risk of loss with respect to an unauthorized payment order . . . ."[163] On remand, the parties settled without briefing the issue. The bank agreed to pay Patco's full unrecovered loss, plus interest,[164] in a case where the losses occurred over a matter of days, well within the 90-day limit of subsection 4A-204(a) or other "reasonable time" within which Patco reasonably could have become aware of the fraud.

In constrast to the cases above, the Eighth Circuit in *Choice Escrow* concluded the bank met its burden of establishing good faith where: (1) the customer was aware that the only time the bank's employees saw the payment order was after the wire cleared its security procedures, (2) the customer was also aware the employees' role was to route payment orders, not check for irregularities, (3) the "payment order was not so unusual that it should have raised eyebrows," as

[160] *Id.* at 214-15.

[161] *Id.* at 214. The First Circuit also acknowledged the Comment to section 4A-102, which states: "Resort to principles of law or equity outside of Article 4A is not appropriate to create rights, duties and liabilities inconsistent with those stated in this Article."

[162] UCC § 4A-204(a) & cmt. 1. What is a reasonable time depends on the facts of the particular case. For example, as explained in the Comment: "If a payment order for $1,000,000 is wholly unauthorized, the customer should normally discover it in far less than 90 days." *Id.,* cmt. 1.

[163] UCC § 4A-204(a) cmt. 1.

[164] Pamela Ryckman, *A Win for Small Businesses in a Bank Fraud Case*, New York Times, (Dec. 12, 2012), available at http://boss.blogs.nytimes.com/2012/12/12/a-win-for-small-businesses-in-bank-fraud-case/ (last visited Oct. 22, 2019). The bank did not pay Patco's attorney's fees, which approximated the $350,000 loss, while incurring an estimated $1 million in fees itself. *Id.*

the amount was not unusual for the customer, and (4) the bank was under no obligation to review the memo line of the payment order.[165]

C. When Customer Is Not the Source of the Security Leak

Another important exception to Article 4A's usual allocation of liability to the customer is found in 4A-203(a)(2). A customer will not bear the loss where it can prove the payment order was not issued by (a) itself or its agent, or (b) someone who gained knowledge of the security procedure (*e.g.*, user ID, password, etc.) from itself or its agent.[166] This provision eliminates negligence of the customer; the issue is whether the customer was the source, "regardless of how the information was obtained or whether the customer was at fault."[167] The exception functions like an affirmative defense in litigation, for which the customer bears the burden of proof under section 4A-203(a)(2).[168] As the Comments note, while the "burden of making available commercially reasonable security procedures is imposed on receiving banks," the corresponding "burden on the customer is to supervise its employees to assure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached."[169] The purpose behind this exception is pragmatic, and based on the reality that criminals have two avenues of attack, against either the bank or the customer.[170]

Historically, electronic payment fraud has originated with the customer, not from hacking into the bank's system.[171] Banks, however, have "always been attractive targets at the center of malicious cyber and fraudulent activity since the internet started to expand worldwide. But the

[165] 754 F.3d at 623-24.
[166] UCC § 4A-203(a)(2).
[167] *Id.*
[168] *Id.*
[169] UCC § 4A-203 cmt. 3.
[170] UCC § 4A-203 cmt. 5.
[171] *See, e.g.,* Rob Garver, *The Cost of Inaction*, U.S. Banker (July 2010), at 11.

threat landscape has been getting worse with nation-states increasingly joining the mix and with the resulting damage escalating, from theft to disruption and destruction."[172] Since 2015 and continuing through the present, there have been numerous, significant cyber attacks against banks around the world, including many carried out by state actors.[173] In March 2017, the G20 finance ministers and centeral bank governors warned that "the malicious use of Information and Communication Technologies (ICT) could . . . undermine security and confidence and endanger financial stability."[174] Banks should therefore be wary that, though their security procedures vis-a-vis customers may be commercially reasonable, their own computers systems could expose them to liability for a loss in the event they are the source of a security information "leak."

D. Article 4A's One-Year Notice Bar

Unless the customer objects to the fraudulent EFTs within one year, its claims against the bank are subject to UCC Article 4A's one-year statute of repose.[175] UCC § 4A-505 provides:

> If a receiving bank has received payment from its customer with respect to a payment order issued in the name of the customer as sender and accepted by the bank, and the customer received notification reasonably identifying the order, the customer is precluded from asserting that the bank is not entitled to retain the payment unless the customer notifies the bank of the customer's objection to the payment within one year after the notification was received by the customer.

[172] Carnegie Endowment for International Peace, *Timeline of Cyber Incidents Involving Financial Institutions*, available at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline (last visited Oct. 23, 2019).

[173] *Id.*; *see, e.g.*, David E. Sanger and Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, New York Times, Feb. 14, 2015, available at https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html (last visited Oct. 23, 2019); Angela Moon, *State-sponsored cyberattacks on banks on the rise*, Reuters, Mar. 22, 2019, available at https://www.reuters.com/article/us-cyber-banks/state-sponsored-cyberattacks-on-banks-on-the-rise-report-idUSKCN1R32NJ (last visited Oct. 23, 2019).

[174] Communiqué, G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17-18 Mar. 2017, at 3, available at https://carnegieendowment.org/files/g20-communique.pdf (last visited Oct. 23, 2019).

[175] UCC § 4A-505 cmt.

As a statute of repose, section 4A-505 does not provide an "affirmative defense . . . often subject to tolling principles," but "extinguishes a plaintiff's cause of action after the passage of a fixed period of time," here, one year.[176]

The duty of the customer to give notice to the bank is triggered by "recei[pt of] notification reasonably identifying the order . . . ."[177] Article 4A does not define "reasonably identify," so the courts have looked to other UCC provisions for assistance. The Second Circuit has approved the borrowing of the "objectively determinable" standard from UCC § 9-108, and held that monthly statements that provided the dollar amount, date, and identification number of wires, as well as the account balance, and monthly wire totals, provided sufficient information from which the customer could identify, and object to, any particular transfer.[178]

Upon receipt of this notification, the customer must notify the bank "of the customer's objection to the payment."[179] Its notice must "identify which, if any, specific payments were disputed," as "vague communication regarding suspicious activity cannot meet this requirement."[180] The California Supreme Court found that the "purpose of the notification requirement is to inform the bank reasonably promptly that the customer believes it is liable for the loss."[181] To satisfy this purpose, the court applied an objective reasonableness test:

> We think the test should be whether, under all of the relevant circumstances, a reasonable bank would understand from the customer's communication that the customer was objecting to what the bank had done in accepting the payment orders or otherwise considered the bank liable for the loss.[182]

[176] Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 597 F.3d 84, 88 n.4 (2d Cir. 2010).
[177] UCC § 4A-505.
[178] *Ma*, 597 F.3d at 91.
[179] UCC § 4A-505.
[180] ReAmerica, S.A. v. Wells Fargo Bank Int'l, 2008 U.S. Dist. LEXIS 30614, *18-19 (S.D.N.Y. Mar. 18, 2008), *aff'd,* 577 F.3d 102 (2d Cir. 2009) (holding customer's communication that it might dispute payments insufficient under § 4A-505).
[181] Zengen, Inc. v. Comerica Bank, 158 P.3d 800, 811 (Cal. 2007).
[182] *Id.* at 812.

Accordingly, the customer must notify the bank not only of specific questioned payments, but that it actually disputes them (or even indicate the bank is liable) in order to satisfy UCC § 4A-505.

E. Liability of the Beneficiary's Bank

Under UCC Article 4A, the liability of a beneficiary's bank is limited to defined, generally unlikely circumstances, for example, where the bank "knows" that the name and account number on the wire transfer order refer to different persons.[183]

The rule is set forth in UCC § 4A-207(b):

> If a payment order received by the beneficiary's bank identifies the beneficiary both by name and by an identifying or bank account number and the name and number identify different persons, the following rules apply:
>
> (1) Except as otherwise provided in subsection (c), if the beneficiary's bank does not know that the name and number refer to different persons, it may rely on the number as the proper identification of the beneficiary of the order. The beneficiary's bank need not determine whether the name and number refer to the same person.
>
> (2) If the beneficiary's bank pays the person identified by name or knows that the name and number identify different persons, no person has rights as beneficiary except the person paid by the beneficiary's bank if that person was entitled to receive payment from the originator of the funds transfer. If no person has rights as beneficiary, acceptance of the order cannot occur.[184]

The application of this rule is illustrated in the recent 11th Circuit case, *Peter E. Shapiro, P.A. v. Wells Fargo Bank, N.A.*,[185] where a law firm "spearfishing" victim sent a $500,000 wire transfer intended for James Messenger, an attorney, but the owner of the account was Chris

[183] UCC § 4A-207. *See, e.g.,* Peter E. Shapiro, P.A. v. Wells Fargo Bank, N.A., 352 F. Supp. 3d 1226, 1223 (S.D. Fla. 2018) (applying UCC § 4A-207 in finding a lack of actual knowledge of a mismatch between the beneficiary name on the payment order and the account name, despite being flagged and then reviewed by an employee for sanctions compliance, but not name discrepancy).

[184] UCC § 4A-207(b).

[185] 2019 U.S. App. LEXIS 35604 (11th Cir. Nov. 27, 2019).

Achebe, a Nigerian citizen. Though (1) Wells Fargo's automated "audit trail reflected that there was a 'possible name mismatch in [credit] party,'"[186] and (2) "the wire was manually screened by an individual person for Office of Foreign Assets Control ("OFAC") compliance purposes," the appeals court noted "no individual person . . . obtained actual knowledge of the possible name mismatch in Shapiro's payment order."[187]

The Official Comment to UCC § 4A-207 explains that:

> Subsection (b) allows banks to utilize automated processing, by allowing banks to act on the basis of the number without regard to the name if the bank does not know that the name and number refer to different persons. "Know" is defined in section 1-201(25) to mean actual knowledge, and section 1-201(27) states rules for determining when an organization has knowledge of information received by the organization. The time of payment is the pertinent time at which knowledge or lack of knowledge must be determined.[188]

"Knowledge" is defined in Revised UCC § 1-202(b) as "actual knowledge. 'Know' has a corresponding meaning."[189] Revised UCC § 1-202(f) states the relevant rules as follows:

> Notice, knowledge, or a notice or notification received by an organization is effective for a particular transaction from the time it is brought to the attention of the individual conducting that transaction and, in any event, from the time it would have been brought to the individual's attention if the organization had exercised due diligence. An organization exercises due diligence if it maintains reasonable routines for communicating significant information to the person conducting the transaction and there is reasonable compliance with the routines. Due diligence does not require an individual acting for the organization to communicate information unless the communication is part of the individual's regular duties or the individual has reason to know of the transaction and that the transaction would be materially affected by the information.[190]

[186] *Id*. at *4.

[187] *Id*. at *4-5.

[188] UCC § 4A-207 cmt. 2.

[189] UCC § 1-202(b). Former UCC § 1-201(25) under Florida law, as applied by the 11th Circuit, similarly provides, "A person "knows" or has "knowledge" of a fact when the person has actual knowledge of it." Fla. Stat. § 671.205(25)(c); 2019 U.S. App. LEXIS 35604, at *9.

[190] UCC § 1-202(f). Former UCC § 1-201(27) in Florida, as applied by the 11th Circuit, is nearly identical. Fla. Stat. § 671.201(27); 2019 U.S. App. LEXIS 35604, at *9.

Finally, UCC § 1-201(27) defines "person" as "an individual, corporation, . . . association, . . . or any other legal or commercial entity."[191]

Applying these principles, the 11th Circuit concluded:

> Considering the clear intention of the statute, which is to allow for the automated processing by banks of a large number of payment orders on a daily basis, while reducing both transaction costs and the potential for clerical error, we easily conclude that Wells Fargo maintained and complied with reasonable routines, and thus exercised due diligence, with respect to the processing of Shapiro's payment order through its automated [system.] In processing the payment order Shapiro originated, it was not unreasonable for Wells Fargo to allow its automated payment system to ignore a potential name mismatch and "rely on the number as the proper identification of the beneficiary of the order." [Wells Fargo] implemented and used an automated system that processed payment orders on the basis of a matching account number alone, ignoring potential name mismatches automatically reflected in the audit trail.[192]

The 11th Circuit further approved Wells Fargo's approach, stating

> Even if Wells Fargo intentionally programmed the automated portions of its MTS system to ignore potential name mismatches. . . "it may rely on the number as the proper identification of the beneficiary of the order" unless and until an individual person conducting the transaction has actual knowledge of a name mismatch or would have had such knowledge had the organization exercised due diligence.[193]

[191] UCC § 1-201(27).

[192] *Id*. at *13-15. The 11th Circuit also rejected the argument that the bank's OFAC review created any issues of fact:

> Wells Fargo, as an organization, did not fail to act with the due diligence required by Article 4A of the UCC by allowing its automated [system] to process [the] funds transfer without escalating information relating to a possible name mismatch to an individual person for review (including the OFAC screener or any other Wells Fargo personnel) [and] the OFAC screener did not have actual knowledge of the potential name mismatch because he reviewed only the original payment order (and not the information generated by the MTS audit trail). Consequently, Wells Fargo still did not fail to act with due diligence in this case because the OFAC screener did not have any material information regarding the name mismatch to "communicate" to other individual persons at Wells Fargo in any event.

Id. at *15-16. The appeals court implicitly rejected that the OFAC reviewer could be considered an "individual conducting that transaction" under UCC § 1-202(f), in which case "due diligence" would require "reasonable routines for communicating significant information to the person conducting the transaction," *id*., including that the name mismatch be communicated to the reviewer. In this regard, the U.S. Treasury Department has advised fraud prevention, anti-money laundering, compliance, cybersecurity and related units within financial institutions to work together to better thwart business email compromise (BEC) cybercrime. *See* Department of the Treasury, Financial Crimes Enforcement Network, Advisory FIN-2019-A005 (July 16, 2019); Department of the Treasury, Financial Crimes Enforcement Network, Advisory FIN-2016-A003 (Sept. 6, 2016).

[193] *Id*. at *4, n.5.

The 11th Circuit, however, also noted,

> One can reasonably question the wisdom of the rule (and the allocation of risk) on which Wells Fargo relied in this case, especially in light of the fact that modern technology probably is capable of easily differentiating between a partial mismatch (e.g., John Doe versus Jon Doe) and a complete mismatch (e.g., James Messenger and Chris Achebe). But, that does not change the fact that Wells Fargo is entitled to rely on the rule as it now exists. . . .[194]

In a recent Virginia case, *AG4 Holding, LLC v. Regency Title & Escrow Servs*, a sender induced by a fraudulent email to send a wire transfer asserted a claim against the beneficiary's bank rather than its own, the receiving bank (presumably because the sender authorized the transfer).[195] The plaintiff sender alleged that the beneficiary's bank opened an account for a nonexistent entity, and thus required acceptance of the order was lacking under UCC § 4A-207(a). That provision states: "Subject to subsection (b) of this section, if, in a payment order received by the beneficiary's bank, the name, bank account number, or other identification of the beneficiary refers to a nonexistent or unidentifiable person or account, no person has rights as a beneficiary of the order and acceptance of the order cannot occur." Subsection (b)(1) provides that "if the beneficiary's bank does not know that the name and number refer to different person, it may rely on the number as the proper identification of the beneficiary of the order. The beneficiary's bank need not determine whether the name and number refer to the same person."[196] The sender did not contend the beneficiary's bank knew the account number and name on the payment order referred to different persons, as required by UCC § 4A-207(b), but rather that, in a claimed case of first impression under UCC § 4A-207(a), which the bank admitted was violated, there could be no acceptance where the beneficiary was nonexistent. Not reaching the question, the court

[194] 2019 U.S. App. LEXIS 35604, at *15, n.9.
[195] 98 Va. Cir. 89, 93 (Va. Cir. Ct. 2018).
[196] UCC § 4A-207(b)(1).

dismissed the claim under UCC § 4A-207 with leave to amend either to address the applicability of subsection 4A-207(b)(1) or to more clearly allege sender's position under subsection 4A-207(a).[197]

In *Song Chuan Tech. (Fujian) Co. v. Bank of Am.*,[198] another fraudulent email case where the recipient was induced to send a wire transfer to an imposter, the court rejected the plaintiff's attempt to assert a claim under UCC § 4A-207 where the payment order was directed to an existing and identifiable account of the imposter, stating: "Section 207 applies only where it is not possible to complete the transfer because the beneficiary cannot be identified—preventing banks from simply keeping funds where it is not possible to complete the transfer."[199] Thus, "Section 207 is inapplicable to the situation alleged here, where a funds transfer is completed to the identified recipient and the sender of funds subsequently realizes the identified recipient was not who he said he was."[200]

In a similar case, *Kafati v. Wells Fargo Bank*[201], a sender brought suit against the beneficiary's bank involving a wire transfer mismatch of names and addresses where the order was directed to an LLC in New Hampshire rather than a person in Florida. The court first dismissed the sender's claims under UCC §§ 4A-202 and 204 because he was not a customer of

[197] 98 Va. Cir. at 98. *But see* New S. Fed. Sav. Bank v. Flatbush Fed. Sav. & Loan Ass'n, 2002 U.S. Dist. LEXIS 20512, at *4-5 (S.D.N.Y. Oct. 24, 2002) (interpreting UCC § 4A-207(a)'s reference "to a nonexistent or unidentifiable person or account" to cover "the case if the payment order gives an account number that does not identify any existing account at the beneficiary bank," explaining: "a number is different from a name. If a number has a digit added or deleted, then it becomes a different number. But if a name has a letter (or a word) added or deleted, then it is not necessarily considered a different name.") (citing Off. Cmt. 1 to UCC § 4A-207; Corfan Banco Asuncion Paraguay v. Ocean Bank*,* 715 So. 2d 967 (Fla. App. 1998) (account number did not identify any existing account); United States v. BCCI Holdings (Luxembourg), S.A.*,* 980 F. Supp. 21, 24 (D.D.C. 1997) (same)); *see also* Tzaras v. Evergreen Int'l Spot Trading, Inc.*,* 2003 U.S. Dist. LEXIS 2707, at *13-15 (S.D.N.Y. Feb. 25, 2003) (UCC § 4A-207(a) requires no more than the name and account number for an "identifiable beneficiary").

[198] 2017 U.S. Dist. LEXIS 34335 (D.S.C. Mar. 10, 2017).

[199] *Id*. at *8 (citations omitted).

[200] *Id.*

[201] 2018 N.Y. Misc. LEXIS 3197 (N.Y. Sup. Ct. Feb. 23, 2018).

the beneficiary's bank as contemplated by those sections.[202] It then rejected claims for misdescription of beneficiary under UCC § 4A-207, stating beneficiary banks "may rely on the bank account number provided to them, unless they actually know that the name on the transfer does not correspond with the bank account number."[203] "Even if that were not the case," that is if the bank had actual knowledge, "small discrepancies, such as the one between Esdras Devalon LLC and Esdras Devalon, are not sufficient to warrant liability under UCC § 4A-207."[204]

F. Common Law Claims

In seeking to recover losses for fraudulent EFTs due to malware, bank customers have asserted various claims at common law, including breach of contract, negligence, gross negligence, negligent misrepresentation, fraud, breach of fiduciary duty, and breach of duty to protect customer's confidential against identity theft, as well as under unfair trade practices statutes. Generally, common law claims will be displaced where they overlap the coverage of, or are "inconsistent" with, Article 4A.

As its Prefatory Note indicates, Article 4A was intended to be comprehensive: "There is no consensus about the juridical nature of a wire transfer and consequently of the rights and obligations that are created. Article 4A is intended to provide the comprehensive body of law that we do not have today."[205] As a result of this careful, comprehensive balancing of interests, "resort to principles of law or equity outside of Article 4A is not appropriate to create rights, duties, and liabilities inconsistent with those stated in this Article."[206]

[202] *Id.* at *8-9.
[203] *Id.* at *10 (citing, *inter alia*, commentary under Regulation J). *See* note 45, *supra.*
[204] *Id.* at *11 (citation omitted).
[205] UCC Article 4A Prefatory Note.
[206] UCC § 4A-102 cmt.

The courts have interpreted these statements generally to preclude common law claims, but there are exceptions.

Illustrative of the general rule, the Second Circuit in *Ma* held that "Article 4A precludes customers from bringing common law claims inconsistent with the statute . . . ."[207] The court examined Article 4A's scope, noting it controlled "how electronic funds transfers are conducted and specifies certain rights and duties related to the execution of such transactions."[208] Next, it compared the allegations in the complaint, finding the "various claims concern alleged misconduct by Merrill Lynch with respect to its execution of electronic transfers."[209] On that basis, it held that Article 4A displaced all common law claims, including breach of contract, breach of fiduciary duty, and negligence.[210]

In *Zengen, Inc.*, the California Supreme Court applied a two-prong test for preclusion: where common law claims would be inconsistent with Article 4A, and "where the circumstances giving rise to the common law claims are specifically covered by" its provisions.[211] The court then examined the negligence and breach-of-contract claims, finding the "gravamen of each" was the "bank should not have accepted and executed the fraudulent payment orders."[212] Because the claims were "squarely within the provisions" of Article 4A, they too were held displaced.[213]

Similarly, in *ADS Associates Group, Inc. v. Oritani Sav. Bank*[214], the New Jersey Supreme Court held that because the case arose in "a setting directly addressed by Article 4A – a bank's

[207] *Ma*, 597 F.3d at 89.
[208] *Id*.
[209] *Id*. at 90.
[210] *See also* Wright v. Citizen's Bank of E. Tenn., 640 Fed. Appx. 401, 409 (6th Cir. 2016) (holding common law claims displaced over bank's one-day delay in correctly completing wire transfer)
[211] 158 P.3d at 808. *See also* Hunter v. Citibank, N.A., 2010 U.S. Dist. LEXIS 61912, *19 (N.D. Cal. Feb. 3, 2010) (claims displaced where "gravamen" was violation of transfer agreements between customer and bank).
[212] *Id*.
[213] *Id*. at 809.
[214] 99 A.3d 345 (N.J. 2014),

acceptance of an order transferring funds from one account held by its customer to another of that customer's accounts," the "Legislature intended Article 4A to constitute the 'exclusive means of determining the rights, duties and liability of the affected parties.'"[215]

Another court finding common law claims for negligence and breach of fiduciary duty displaced, held that "unless altered by express agreement between [originator] and [receiving bank, the bank's] duties to [the originator] are only those provided in Article 4A" where the originator alleged the receiving bank failed to issue a performance bond as required under a purchase agreement between the originator and beneficiary.[216]

Other courts have found exceptions to the general rule of preclusion. For example, the Eleventh Circuit declined to find displaced common law claims based on allegations the bank accepted funds "when it knew or should have known that the funds were fraudulently obtained," because Article 4A is "silent" on the issue.[217] The same reasoning has been applied to permit claims for unjust enrichment and conversion against beneficiaries.[218]

Negligence claims arising from a beneficiary bank's erroneously informing an originator that the transfer had not been received, however, were held displaced, as "[section 4A-404(b)] requires a bank to follow instructions to notify the beneficiary when its accepts a payment order, and provides a remedy if the bank does not do so."[219]

[215] 99 A.3d at 359 (quoting UCC 4A-102 cmt. 1.).

[216] Atl. Energy Group Ltd. V. Ne. Direct Corp., 53 F. Supp. 3d 810, 816 (D.S.C. 2014).

[217] Regions Bank v. Provident Bank, Inc., 345 F.3d 1267, 1275 (11th Cir. 2003).

[218] *See, e.g.,* Frankel-Ross v. Congregation Ohr Hatalmud, 2016 U.S. Dist. LEXIS 128342, at *20-21 (S.D.N.Y. Sep. 13, 2016) (unjust enrichment); Baerg v. Ford, 2016 Ky. App. LEXIS 19, *8-11 (Ky. App. Feb. 19, 2016) (conversion); Koss Corp. v. Am. Express Co., 309 P.3d 898, 905-10 (Ariz. App. 2013) (conversion, aiding and abetting fraud, aiding and abetting breach of fiduciary duty).

[219] Moody Nat'l Bank v. Texas City Dev. Ltd., Co., 46 S.W.3d 373, 378 (Tex. App. 2001).

A developing line of cases has allowed certain common law claims based on prior or subsequent bank conduct. Several courts have held negligence claims based on prior account opening not preempted by the UCC. In *Gilson v. TD Bank*,[220] the court observed that plaintiffs'

> negligence claim is based on the TD Bank's constructive knowledge of the fraudulent nature of the wire transfers. Had TD Bank followed its security procedures, Plaintiffs claim, the Bank would have known that Stein was not authorized to open the subject bank accounts, much less wire transfer money in and out of them. While the Court agrees with Plaintiffs' argument on this point, it finds that they advance an even stronger argument for denying Article 4A preemption. As Plaintiffs point out, the basis for their negligence claim extends beyond TD Bank's conduct with regard to the wire transfers into and out of the accounts. Indeed, Plaintiffs' negligence claim centers on the Bank's allegedly negligent and reckless conduct with regard to opening the accounts. Plaintiffs' Second Amended Complaint alleges that TD Bank acted with gross negligence and recklessness in numerous ways during the account openings, and the record shows a genuine issue of material fact on this issue. Plaintiffs have come forward with evidence that TD Bank deviated from its standard account opening procedures by not receiving a filing receipt or partnership agreement for G&C. Moreover, Plaintiffs evidence shows that TD Bank failed to notice inconsistencies on the account opening documentation for the G&C accounts, such as the discrepancy between the account address and phone number, which were Stein's, and Stein's professed limited role as investment_accounts were opened without proper authorization or authority allowing the individual who opened the accounts to transfer substantial funds out of the accounts for his own benefit.[221]

Similarly, in *Anderson v. Branch Banking & Trust Co*.,[222] the court recognized, "Plaintiffs' accusations with respect to BankAtlantic's lack of care exceed simple objections to unauthorized funds transfers. Instead, they extend to the imprudent handling of the account openings. . . . Because Plaintiffs' negligence theory is not inconsistent with the rights, duties, and obligations under the U.C.C., Plaintiffs' claim is not displaced."[223]

[220] 2011 U.S. Dist. LEXIS 7805 (S.D. Fla. Ja. 27, 2011).
[221] *Id.* at *26-27.
[222] 119 F. Supp. 3d 1328 (S.D. Fla. 2015).
[223] *Id*. at 1358.

As for subsequent conduct, in *Schlegel v. Bank of America*[224] the Virginia Supreme Court distinguished common law claims arising from unauthorized payment orders from claims based on the bank's subsequent freezing of funds. As in *Zengen*, the court found that Article 4A's allocation of liability for unauthorized payment orders displaced the common law claims based on the bank's acceptance of the payment order.[225] But the court held the bank's actions in freezing the funds in the account where they had been transferred, and refusing to return them to the customer, was "not a situation covered by any of the particular provisions of [Article 4A]," and thus common law claims for conversion and breach of contract were not displaced.[226]

Another recent Virginia case likewise held it "is not unambiguously clear that Article 4A preempts" a sender's common law negligence claim against a beneficiary bank that agreed to freeze the account of its account holder into which a wire transfer was made after the sender was induced by a fraudulent email.[227] The court reasoned that the bank's promise to freeze the account could be considered an agreement to shift liability under UCC §§ 4A-211 and 4A-212, and required plaintiffs to amend their complaint to "allege facts which support their proposition the claim is not preempted."[228]

Similarly, in *3T Oil & Gas Servs., LLC. v. JP Morgan Chase Bank, N.A.*,[229] a fraudulent email case where the plaintiff was induced into sending a wire transfer to an imposter, the plaintiff brought suit against the beneficiary's bank alleging a subsequent negligent misrepresentation. The court rejected the bank's argument that the claim was displaced:

> [Plaintiff's] negligent misrepresentation claim in this case is similarly not based on the wire transfer itself, or on any claim that [the bank] mishandled the wire transfer,

[224] 628 S.E.2d 362, 367-68 (Va. 2006).
[225] *Id.* at 368.
[226] *Id.*
[227] *AG4 Holding, supra,* 98 Va. Cir. at 101.
[228] *Id.*
[229] 2018 U.S. Dist. LEXIS 177169 (W.D. Tex. Oct. 16, 2018).

> but rather is based on representations made by [the bank] *after* the wire transfer was completed. Specifically, [the Plaintiff] alleges that after the wire transfer was completed, [the bank] informed [it] that the funds had been flagged and that [the bank] would not permit the funds to be moved out of the bank. [Plaintiff] contends that it relied on these representations and did not seek a court order to prevent [the bank] from releasing the funds. None of these allegations fall within the provisions of [UCC Article] 4A. Accordingly, [Plaintiff's] negligent misrepresentation claim is not preempted by [UCC Article] 4A.[230]

In a recent case arising from fraudulent ACH transactions, the court dismissed all non-UCC Article 4A counts, including breach of contract and violation of federal banking statutes and regulations.[231] Addressing the contract claim, the court found the account holders were not parties to any relevant electronic banking agreement with the bank; rather, the agreements were between the account holders' related entity and the bank.[232] In the absence of any applicable agreement identifying an agreed security procedure, however, the bank seemingly would be subject to strict liability for any unauthorized payments.[233]

In sum, the question of displacement turns on the relationship between the acts underlying the common law claim and the "rights and obligations" created by Article 4A. The more those acts resemble a situation covered by Article 4A, the more likely they are to be held displaced, and *vice versa.*

[230] *Id*. at *8-9 (emphasis in original.)

[231] Federal Ins. Co. v. Benchmark Bank, 2018 U.S. Dist. LEXIS 11152 (S.D. Ohio Jan. 24, 2018).

[232] *Id*. at *13-15.

[233] *See* UCC §§ 4A-202(b), 4A-204(a).

G. Interbank Liability for Fraudulent Electronic Funds Transfers

The federal banking regulators warn banks to be alert for suspicious electronic deposits: "Money mule activity is essentially electronic money laundering addressed by the Bank Secrecy Act and Anti-Money Laundering Regulations. Strong customer identification, customer due diligence, and high-risk account monitoring procedures are essential for detecting suspicious activity, including money mule accounts."[234] Oftentimes a receiving bank may be able to recover a portion of the fraudulent EFTs, depending on how quickly it or its customer discovered the fraud, on the cooperation of the bank receiving the stolen funds (the "beneficiary bank" under Article 4A, or receiving depository financial institution ("RDFI") for ACH transfers under NACHA[235] rules), and on whether the criminal has already withdrawn the stolen funds. Apart from such voluntary cooperation and the developing line of cases discussed above that allow common law claims based on prior or subsequent bank conduct, a customer and its bank generally have little recourse against beneficiary banks or RDFIs.

In the case of ACH transfers, under the NACHA Operating Rules the customer's bank, the originating depository financial institution ("ODFI") warrants, "to each RDFI and ACH Operator" that the "entry has been properly authorized by the Originator and the Receiver."[236] ODFIs may make return requests for erroneous entries under Section 2.12.[237] The period for requesting a return entry on an ACH transaction is five days.[238] An ODFI is required to indemnify each RDFI and ACH Operator from any claims and losses resulting from reversing any erroneous entry.[239]

[234] FDIC Special Alert, SA-185-2009, Fraudulent Work-At-Home Funds Transfer Agent Schemes (Oct. 29, 2009).
[235] *See* note 44, *supra*.
[236] NACHA Operating Rules, §§ 2.4.1 and 2.4.1.1 (2019).
[237] *Id*. at § 2.12 (2019).
[238] *Id*. at § 2.9.1 (must be made to the ACH Operator "in such time as to be Transmitted or made available to the RDFI within five Banking Days following the Settlement Date of the Erroneous Entry.")
[239] *Id*. at § 2.9.1 (2019).

Unless displaced by Article 4A, as discussed above, a customer or its bank potentially may also have common law claims against the beneficiary bank under certain circumstances. For example, in *Regions Bank v. Provident Bank, Inc.*,[240] the 11th Circuit held:

> 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. Therefore, a provision of state law that requires a receiving or beneficiary bank to disgorge funds that it knew or should have known were obtained illegality when it accepted a wire transfer is not inconsistent with the goals or provisions of Article 4A. . . . . Interpreting Article 4A in a manner that would allow a beneficiary bank to accept funds when it knows or should know that they were fraudulently obtained, would allow banks to use Article 4A as a shield for fraudulent activity. It could hardly have been the intent of the drafters to enable a party to succeed in engaging in fraudulent activity, so long as it complied with the provisions of Article 4A[241]

As also discussed above, the 11th Circuit recently sidestepped *Regions Bank* in *Peter E. Shapiro, P.A. v. Wells Fargo Bank, N.A,*[242] concluding that a beneficiary bank complied with Article 4A notwithstanding that an automated audit trail showed a possible name mismatch[243] and the wire was manually screened for OFAC compliance, because "no individual person . . . obtained actual knowledge of the possible name mismatch."[244] As a result, the appellate court held that Article 4A preempted a common law negligence claim based on the funds transfer.[245]

[240] 345 F.3d 1267 (11th Cir. 2003).

[241] *Id*. at 1276.

[242] 2019 U.S. App. LEXIS 35604 (11th Cir. Nov. 27, 2019).

[243] *Id*. at *4.

[244] *Id*. at *4-5.

[245] *Id*. at *18-20.

V. THIRD-PARTY RECOVERY AGAINST AUDITORS

Auditors have long faced exposure for failing to conduct audits in conformity with Generally Accepted Auditing Standards and the applicable audit engagement agreement, including in cases involving embezzlements.[246]

In recent decades, embezzlement cases against auditors have also involved theft by EFTs, primarily fraudulent wire transfers.[247] Those embezzlement schemes often take place over extended periods of several years or more. In contrast, fraudulent EFTs conducted via cybercrime are generally discovered quickly, limiting cybercrime schemes to a short duration. In the event fraudulent EFTs due to cybercrime are carried out over an extended period subject to annual audit, claims potentially would lie against auditors in the same way as traditional embezzlement losses.

[246] *See, e.g.*, National Surety Corp. v. Lybrand, 9 N.Y.S.2d 554 (1939); Vigilant Ins. Co. v. Deloitte & Touche, LLP, 2008 Conn. Super. LEXIS 1520 (Conn. Super. June 12, 2008).

[247] *See, e.g.,* Colonial BancGroup Inc. v. Pricewaterhouse Coopers LLP, 2017 U.S. Dist. LEXIS 221182 (M.D. Ala. Dec. 28, 2017); Deloitte Tax, LLP c. Amedisys, Inc., 2018 La. App. LEXIS 1109 (La. App. May 16, 2018); County of Alcona v. Robson Accounting, Inc., 2013 Mich. App. LEXIS 1532 (Mich. App. Sept. 24, 2013); Vigilant Ins. Co. v. Deloitte & Touche, LLP, 2009 Conn. Super. LEXIS 2796 (Conn. Super. Oct. 26, 2009).