

The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION

March 2025

Editor's Note: The World of Banking
Victoria Prussen Spears

Achieving Financial Stability and Resilience: How China Could Learn from the United States and the United Kingdom in Building a Financial Safety Net – Part I
Lerong Lu and Ci Ren

Bankers Worldwide: You May Not Be Interested in Export Controls, But They Are Interested in You
Cari Stinebower, Carl Fornaris, Richard Weber, Juan Azel, Dainia Jabaji and Tony Busch

Africa's Potential for Sustainable Sovereign Finance
Barthélemy Faye, Christophe Wauters and Pap Diouf

Consumer Financial Protection Bureau Finalizes New Federal Supervision of Certain Providers of Digital Wallets, Payment Apps
Eamonn K. Moran, Christopher M. Phillips, Cynthia G. Burnside and Jennifer A. Connors

Burdensome Proposed Federal Deposit Insurance Corporation For-The-Benefit-Of Account Rule Looms Large for Banks and FinTechs
Juan Azel, Carl Fornaris, Monica Lopez-Rodriguez and Julia Lagnese

I've Read the U.C.C. Amendments So You Do Not Have To – Part I
Mercedes Kelley Tunstall

THE BANKING LAW JOURNAL

VOLUME 142

NUMBER 3

March 2025

| | |
|--|-----|
| Editor's Note: The World of Banking Victoria Prussen Spears | 111 |
| Achieving Financial Stability and Resilience: How China Could Learn from the United States and the United Kingdom in Building a Financial Safety Net – Part I Lerong Lu and Ci Ren | 114 |
| Bankers Worldwide: You May Not Be Interested in Export Controls, But They Are Interested in You Cari Stinebower, Carl Fornaris, Richard Weber, Juan Azel, Dainia Jabaji and Tony Busch | 123 |
| Africa's Potential for Sustainable Sovereign Finance Barthélemy Faye, Christophe Wauters and Pap Diouf | 130 |
| Consumer Financial Protection Bureau Finalizes New Federal Supervision of Certain Providers of Digital Wallets, Payment Apps Eamonn K. Moran, Christopher M. Phillips, Cynthia G. Burnside and Jennifer A. Connors | 134 |
| Burdensome Proposed Federal Deposit Insurance Corporation For-The-Benefit-Of Account Rule Looms Large for Banks and FinTechs Juan Azel, Carl Fornaris, Monica Lopez-Rodriguez and Julia Lagnese | 140 |
| I've Read the U.C.C. Amendments So You Do Not Have To – Part I Mercedes Kelley Tunstall | 145 |

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Matthew T. Burke at (800) 252-9257
Email: matthew.t.burke@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call or email:

Customer Services Department at (800) 833-9844
Outside the United States and Canada, please call (518) 487-3385
Fax Number (800) 828-8341
Customer Service Website <http://www.lexisnexis.com/custserv/>

For information on other Matthew Bender publications, please call

Your account manager or (800) 223-1940
Outside the United States and Canada, please call (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)

ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

This publication is designed to provide authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Matthew Bender, the Matthew Bender Flame Design, and A.S. Pratt are registered trademarks of Matthew Bender Properties Inc.

Copyright © 2025 Matthew Bender & Company, Inc., a member of LexisNexis. All Rights Reserved.

No copyright is claimed by LexisNexis or Matthew Bender & Company, Inc., in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW  BENDER

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

CARLETON GOSS

Partner, Hunton Andrews Kurth LLP

DOUGLAS LANDY

White & Case LLP

PAUL L. LEE

Of Counsel, Debevoise & Plimpton LLP

MICHAEL D. LEWIS

Partner, Sidley Austin LLP

TIMOTHY D. NAEGELE

Partner, Timothy D. Naegele & Associates

STEPHEN J. NEWMAN

Partner, Steptoe & Johnson LLP

ANDREW OLMEM

Partner, Mayer Brown LLP

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2025 Reed Elsevier Properties SA., used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

Bankers Worldwide: You May Not Be Interested in Export Controls, But They Are Interested in You

*By Cari Stinebower, Carl Fornaris, Richard Weber, Juan Azel, Dainia Jabaji and Tony Busch**

In this article, the authors examine the expectations articulated by a six-page guidance statement to financial institutions regarding best practices under the Export Administration Regulations released recently by the U.S. Department of Commerce's Bureau of Industry and Security.

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) has released a six-page guidance statement (the Guidance) to financial institutions (FIs) regarding best practices under the Export Administration Regulations (EAR).¹ Many FIs are well acquainted with U.S. economic sanctions and anti-money laundering laws and regulations, but few have invested in more than the most rudimentary export controls compliance functions. The Guidance highlights the risks to and expectations of FIs under the EAR and applies equally to both U.S. and foreign banks and other FIs engaging in cross-border activity. Below, we provide the context, risks, and, most importantly, our thoughts on the expectations that the Guidance articulates.

THE STEADY MARCH TOWARD GREATER EXPORT CONTROLS EXPECTATIONS OF FINANCIAL INSTITUTIONS

While the bases for regulation of FIs under the EAR have been on the books for many years, FIs have not traditionally had to contend with intense scrutiny by BIS. Russia's further invasion of Ukraine, as in many areas of trade regulation, prompted greater collaboration and creativity between and among U.S. and partners' international trade agencies. In the first-ever joint alert by BIS and FinCEN in 2022,² the agencies requested FIs use the key term "FIN2022-RUSSIABIS" in Suspicious Activity Reports (SARs) for suspected Russia-related export controls evasion, and provided a list of 16 "commodities

* The authors, attorneys with Winston & Strawn LLP, may be contacted at cstinebower@winston.com, cforanaris@winston.com, rweber@winston.com, jazel@winston.com, djabaji@winston.com and abusch@winston.com, respectively.

¹ <https://www.bis.gov/media/documents/guidance-financial-institutions-best-practices-compliance-export-administration>.

² <https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf>.

of concern.” In May 2023, BIS and FinCEN provided supplemental guidance³ on the Russia-related effort, and in a November 2023 joint guidance,⁴ the agencies provided the key term “FIN-2023-GLOBALEXPORT” for inclusion on SARs for all non-Russia-related suspected evasion. Each of those joint notices provides significant commentary on potential red flags FIs should look out for, to supplement the non-exhaustive list at 15 C.F.R. Part 732 Supplement No. 3.⁵ Finally, BIS worked with allies to construct the Common High Priority List (CHPL) in February 2024, a list of items by six-digit Harmonized Tariff Schedule code that are at a high risk for diversion to Russia.⁶

EXTRATERRITORIAL SCOPE OF U.S. EXPORT CONTROLS

The EAR and other U.S. export controls focus primarily on the global movement or transmission, physically or electronically, of goods, software, and technology/technical data (collectively, Items). In addition to exports from the United States, subsequent “reexports” or “in-country transfers” occurring wholly outside the United States remain within BIS’s jurisdiction, and even some Items produced outside the United States can come under BIS’s jurisdiction due to the incorporation of more than a de minimis amount of U.S.-origin controlled content or due to being produced using U.S. software, technology, or equipment under certain circumstances. Such Items and transactions are referred to as “subject to the EAR.” Interestingly, the Guidance casually included one of its most explicit written statements ever on EAR jurisdiction over foreign-produced microelectronics and integrated circuits (i.e., semiconductors), BIS stated that “nearly all” such Items fall under its jurisdiction.

It is also worth noting that the EAR and U.S. military export controls under the International Traffic in Arms Regulations (ITAR) contain restrictions on certain “activities” or “defense services,” respectively, by U.S. persons. Even non-U.S. persons activities and services occurring outside the United States, regardless of currency, can be regulated, as illustrated by examples such as General Prohibition Ten (GP 10) under the EAR, or arms-brokering controls

³ <https://www.bis.doc.gov/index.php/documents/enforcement/3272-fincen-and-bis-joint-alert-final-508c/file>.

⁴ https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf.

⁵ <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-732/appendix-Supplement%20No.%203%20to%20Part%20732>.

⁶ <https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items>.

imposed on non-U.S. persons owned or controlled by U.S. persons under the ITAR.

EXPORT CONTROLS RISKS TO FINANCIAL INSTITUTIONS

The primary export controls risk to FIs is a GP 10 violation. GP 10 prohibits “[p]roceeding with transactions with knowledge that a violation has occurred or is about to occur.” Specifically, no person (including individuals and entities, domestic and foreign) may:

sell, transfer, export, reexport, *finance*, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, *or otherwise service*, in whole or in part, *any item subject to the EAR* and exported, reexported, or transferred (in-country) or to be exported, reexported, or transferred (in-country) *with knowledge that a violation* of the Export Administration Regulations, the Export Control Reform Act of 2018, or any order, license, license exception, or other authorization issued thereunder *has occurred, is about to occur, or is intended to occur* in connection with the item.⁷

“Knowledge” under the EAR includes not only actual knowledge but also “an awareness of a high probability of [a circumstance’s] existence or future occurrence” where “[s]uch awareness is inferred from evidence of the conscious disregard of facts known” or a “willful avoidance” of facts.

The Guidance also highlights the EAR’s prohibitions on certain “activities” by U.S. persons (which include foreign branches of U.S. entities). These controls can prohibit U.S. persons from facilitation activities relating to some Items not “subject to the EAR.”

Most EAR violations are subject to civil penalties under the of the Export Control Reform Act of 2018 (ECRA) of the greater of \$364,992 and twice the transaction value. While there is a “knowledge” requirement for some EAR violations – such as GP 10 – the EAR operate a strict liability regime (no intent required) for civil violations. Criminal violations under ECRA are subject to penalties of up to \$1 million, imprisonment for 20 years, or both, per violation.

EXPECTATIONS OF FINANCIAL INSTITUTIONS ARISING FROM THE GUIDANCE

The Guidance appears calculated to push FIs’ export controls compliance postures forward through onboarding and periodic heightened due diligence (HDD) and targeted “real-time” compliance measures. Additionally, the Guidance aims to enlist FIs in BIS’s intelligence-gathering activities through

⁷ 15 C.F.R. § 736.2 (emphases added).

post-transaction red flag identification, mitigation, and reporting. While the Guidance appears to have been written with wire transfers in mind, where FIs have exceedingly little access to information or ability to identify red flags in real time, it does not necessarily illuminate BIS's thinking on how the obligations might increase in a trade finance transaction – such as issuance of a letter of credit – where the FI is still providing an ancillary service to the underlying export, reexport, or transfer, albeit more actively involved than in a wire transaction.

Periodic Heightened Due Diligence

At onboarding and periodically thereafter, the Guidance asks FIs to conduct HDD for both list-based and CHPL Russia evasion reasons:

- *List-Based*: The Guidance asks FIs to “heavily weigh” a customer’s presence on a BIS restricted-party list when determining the EAR violation risk profile of the customer. While FIs, including many foreign FIs, are already comfortable screening against economic sanctions lists, such as the Specially Designated Nationals and Blocked Persons List (SDN List), export controls lists present a different set of restrictions that depend less on the nexus to a U.S. person and instead rely more on the U.S. jurisdiction over the underlying Item. Such lists include the BIS Entity List, Military End-User (MEU) List, Military-Intelligence End-User (MIEU) List, Denied Persons List, and Unverified List, as well as the Directorate of Defense Trade Controls’ Debarred Parties List.
- *Russia Evasion*: The Guidance asks FIs to employ publicly available trade intelligence⁸ to determine whether customers’ past transactions (looking back to 2023) have been identified as involving CHPL Items going to Russia. Consistent with BIS’s increasing separation of the entity-based and location-based screening functions with its first-ever designation of addresses (with no party names) on the Entity List in June,⁹ the Guidance indicates addresses with a publicly available CHPL Item history deserve close scrutiny. The Guidance also indicates reviews of customers’ customers may even be appropriate, depending on the circumstances.

If one or both are triggered, and if the Items are “subject to the EAR,” the Guidance recommends FIs require their customer to certify that it:

⁸ https://www.bis.gov/sites/default/files/files/Guidance-for-Complying-with-BIS-Letters-Identifying-Transaction-Parties-of-Diversion-Risk_v8.pdf.

⁹ <https://www.bis.gov/press-release/department-commerce-announces-additional-export-restrictions-counter-russian>.

- Has sufficient controls in place to comply with the EAR, including screening transactions against lists of persons subject to BIS's end-user restrictions;
- Exercises HDD for exports, reexports, or transfers to destinations subject to BIS-administered embargoes or broad trade restrictions, such as Russia; and
- Engages in HDD processes for Items included on the Commerce Control List or the CHPL.

“Real-Time” Screening

In recognition of the extreme difficulty of “real-time” screening for export controls purposes, especially in the case of wire transactions where a FI might process millions of transfers in a day, the Guidance states that as a baseline starting point, “BIS does *not* expect FIs to engage in real-time screening of parties to a transaction to prevent violations of GP 10.”

However, the exception to that default under the Guidance is that FIs perform real-time screening of the ordering customer and the beneficiary customer in a SWIFT message involving cross-border payments for a targeted set of problematic transaction parties under the EAR, including parties on the:

- Denied Persons List;
- MIEU List (contrast with the much larger MEU List); and
- Entity List, but only if designated as a footnote 3 or 4 entity, or subject to nuclear, chemical and biological, and/or rocket systems or unmanned aerial vehicle end-use license review policies (collectively, with the Denied Persons List and the MIEU List, the FI Real-Time Screening Lists).

BIS is apparently comfortable with FIs continuing to process, in the very first instance, cross-border wires for “less” risky but otherwise problematic parties under the EAR (e.g., all persons on the Unverified List or the MEU List who are not otherwise listed in the FI Real-Time Screening Lists above). Of course, BIS’s “real-time” screening expectations are in addition to and do not supplant all the pre-existing economic sanctions and other screening an FI is already performing.

Post-Transaction Reviews

The Guidance instructs that FIs should not consider the exercise over after a transaction clears. The onboarding and real-time screening notwithstanding, BIS also expects FIs to conduct risk-based post-transaction reviews and to mitigate red flags identified or else risk incurring “knowledge” for purposes of

GP 10 for any future transactions involving the relevant party. The Guidance suggests the reviews would include resolving matches to parties on the full suite of U.S. export controls restricted-parties lists (and not just the FI Real-Time Screening Lists above). Following up on such negative screening results for mere wire transfers could grind the system to a halt or increase costs beyond tolerable levels.

The Guidance also highlights red flags involving refusals by a customer to provide information upon a request, identification of addresses co-located with a party on the Entity List or SDN List, and/or last-minute changes in payment routing away from a country of concern as red flags that cannot arise twice for the same party without satisfactory mitigation by the FI.

Most likely, BIS intends to target foreign FIs it has reason to believe are continuously processing questionable transactions for enforcement. However, U.S. FIs or foreign FIs that closely adhere to U.S. regulatory requirements will have a particularly uncomfortable dilemma deciding how far to go (and how much money and time to spend) on satisfying BIS's expectations.

THE UPDATED BIS VOLUNTARY SELF-DISCLOSURE PROCESS

The Guidance should be viewed in the context of recent policy announcements and regulatory changes by the BIS Office of Export Enforcement (OEE). In particular, on September 12, 2024, BIS memorialized¹⁰ in the EAR how the OEE will process voluntary self-disclosures (VSDs) involving minor or technical violations within 60 days with either a no-action or warning letter. The amendments also describe a more abbreviated narrative requirement for such minor/technical violations, endorse bundling into quarterly submissions, and clarify that disclosure of other persons' conduct leading to an enforcement counts as "exceptional cooperation" for any future violations by the discloser. FI compliance departments should become familiar with the EAR's VSD process at 15 C.F.R. § 764.5, as it may become standard practice to routinely disclose.

CONCLUSION

FIs have never known more clearly where they stand with BIS than they do now. But with that clarity comes increased expectations. Given its already stretched resources, BIS likely does not want to be in the business of constantly pursuing FIs – particularly well-behaved ones – for GP 10 violations, as opposed to the underlying transaction parties BIS already investigates.

However, it will behoove FIs to build an additional layer into their export controls compliance and establish a practice of periodically feeding BIS,

¹⁰ <https://www.bis.gov/press-release/commerce-implements-regulatory-changes-voluntary-self-disclosure-process-and-penalty>.

through VSDs, a healthy diet of investigation-worthy transactions. Showing robust compliance through documented processes and VSDs may be even more important for foreign FIs than domestic ones as the former are probably more likely, depending on a variety of factors, to be targeted for heavy-handed enforcement or sanctions.