CSinsiderNewsletter
A U.S. Company Serving U.S. Financial Institutions
March 2020

Compliance Systems' Coronavirus COVID-19 Response

Compliance Systems continues to stay informed about developments surrounding the coronavirus (COVID-19). We have a team dedicated to daily monitoring and assessment of the situation to determine our best strategies as an organization and how we can serve you during this unpredictable period.

In this unprecedented time, we want you to have the tools in hand to be as flexible as possible to continue generating new business and serving your existing customers.

If you use Simplicity Runtime as part of your Compliance Systems solution:

- You can use Runtime Deal Maker for no cost for 90 days to unlock your transaction documentation for modification. We know that you need to be flexible in order to work with your customers to close deals. Runtime Deal Maker lets you do that. For information, please contact support@compliancesystems.com or call 800-968-8522. Our Deal Maker offer is described in the press release available here.
- You can perform loan modifications as necessary to commercial lines of credit to adjust terms for your customers. You can find procedural information in your platform **Job Aids** sub-forum on the Community Lounge.
- You can launch Runtime directly from Simplicity Configuration in the event that you cannot launch it from your platform system. You can find procedural information in the **Simplicity Runtime News & Updates** forum on the Community Lounge.

Note that Simplicity Runtime may not be part of your platform's integration with Compliance Systems.

Our Product team has collected information about the potential impact of COVID-19 on consumer lending. The team has also put together information on the extension of the federal income tax filing deadline. You can find both posts in the **Regulatory & Industry Updates** forum on the Community Lounge.

We have created a **COVID-19 Business Knowledge Exchange** forum on the Community Lounge. This moderated forum is for all clients who are looking for business information related to COVID-19 developments affecting our industry. Please join the conversation.

We will continue to keep you informed as we determine how we can serve you best. You can find updates about our business resiliency plans by visiting the CUNA Mutual website.

Thank you for your continued partnership and trust.

Regulation CC Adjusts Dollar Amounts for Inflation

The Bureau of Consumer Financial Protection and the Board of Governors of the Federal Reserve System (Agencies) are amending Regulation CC to adjust the dollar amounts under the Expedited Funds Availability Act (EFA Act) for inflation. These amendments are effective July 1, 2020.

The EFA Act and Regulation CC contain the following specified dollar amounts that are impacted by these amendments:

1. "Minimum Amount" – The minimum amount of deposited funds that banks must make available for withdrawal by opening of business on the next day for certain check deposits
   - This was amended from $200 to $225[1]
2. "Cash Withdrawal Amount" – The amount of deposited funds a bank must make available when using the EFA Act's permissive adjustment to the funds availability rules for withdrawals by cash or other similar means
   - This was amended from $400 to $450[2]
3. "New Account Amount" – The amount of funds deposited by certain checks in a new account that are subject to next day availability
   - This was amended from $5,000 to $5,525[3]
4. "Large Deposit Threshold" - The threshold for using an exception to the funds availability schedules if the aggregate amount of checks on any one banking day exceeds the threshold amount
   - This was amended from $5,000 to $5,525[3]
5. "Repeatedly Overdrawn Threshold" – The threshold for determining whether an account has been repeatedly overdrawn
   - This was amended from $5,000 to $5,525[3]
6. The civil liability amount for failing to comply with the EFA Act's requirements
   - This was amended from $1,000 to $1,100 for individual actions (must not be less than $100 or greater than $1,100) and from $500,000 to $525,500 (total recovery in any class action or series of class actions arising out of the same failure to comply)[4]

The EFA Act will adjust these amounts at five-year intervals. The next adjustments after July 1, 2020, will be effective July 1, 2025 and July 1 of every fifth year after 2025. The Agencies will measure inflation by July's Consumer Price Index for Urban Wage Earners and Clerical Workers and will be rounded to the nearest multiple of $25.

Additionally, there are no changes to Regulation CC's change-in-terms notice requirement despite financial institutions' concerns of disproportionate costs and burdens. The current statutory change-in-terms provision remains the same, which requires a financial institution to send a written notice to consumer account owners at least 30 days before a financial institution implements a change, and any change that expedites the availability of such funds must be disclosed no later than 30 days after implementation.

What Financial Institutions Should Be Doing

Financial institutions should consider taking the following actions prior to the July 1 effective date:

- Create a timeline for when they should implement these changes, especially if they choose to implement these changes prior to July 1, 2020.
- Update the Funds Availability and Hold Notice disclosures to ensure that the adjusted dollar amounts are in effect by July 1, 2020. Financial institutions may also have to update any other documentation that references these dollar amounts, such as postings in their lobbies.
- Prepare the change-in-terms notice to send to account owners. Because more money will be made available to account owners faster, financial institutions must send the notice no later than 30 days after the effective date. The notice can be made electronically, pursuant to the E-Sign Act, or it can be included with the monthly statement.
- Update their policies, procedures, and core systems to make sure they reflect and account for the applicable dollar adjustments, such as review of the financial institution's procedure for placing and reviewing holds. Employee training should also be conducted on these new thresholds.

1 229.10(c)(1)(vii)
2229.12(d)
3 229.13(a), 229.13(b), and 229.13(d)
4 229.21(a)

SECURE ACT 2019

The SECURE Act of 2019 (SECURE Act) was passed December 20, 2019 with an effective date of January 1, 2020 and since then, the retirement industry has been trying to catch up and is waiting for guidance from the IRS. As a recap, a few of the important changes that are most impactful to IRA providers are listed below:

Funding Flexibility - A Traditional IRA owner can now fund their IRA past the age of 70 ½ if they have earned income.

Required Minimum Distributions (RMDs) - The SECURE Act extended the required age to take required minimum distributions from 70 ½ to 72. Owners who obtained the age of 70 ½ before December 31, 2019 are still required to begin taking RMDs in 2020.

Beneficiary Options - The SECURE Act also provides that most non-spouse beneficiaries are now required to withdraw the entirety of their share of an inherited IRA within 10 years, which removes the option of spreading distributions over a life expectancy.

Childbirth and Adoption – IRA owners are now able to take a penalty-free withdrawal of up to $5,000 for childbirth or adoption expenses. An IRA owner is also eligible to repay the funds that were withdrawn but not used back into the IRA.

Since the signing of the bill, many have been anxiously awaiting guidance. There has been some guidance regarding a few of these changes from the IRS, but for the most part, we are still in a waiting pattern.

Guidance Regarding Erroneous RMD Statements
On January 24, 2020, the IRS issued IRS Notice 2020-06 which provides relief for reporting RMDs for IRAs for 2020 due to the short amount of time that financial institutions had to update their systems after the enactment of the SECURE Act. Based on the SECURE Act, individuals who turned 70 ½ in 2020 are not required to take an RMD in 2020. However, some financial institutions may have already sent these individuals their RMD notices or could not make changes to their notices to reflect these recent law changes. Notice 2020-06 provides that if a RMD notice was provided to an individual who turns 70 ½ in 2020, under the SECURE Act would no longer need to take an RMD in 2020. The IRS will not consider such statements to be incorrect, provided that the financial institution notifies the IRA owner no later than April 15, 2020 that no RMD is due for 2020.

Updated Documents and Instructions
On February 19, 2020, the IRA posted the final version of the 2020 Instructions for Forms 1099-R and 5498. The instructions include guidance as it relates to the Qualified Birth and Adoptions Distributions and the repayment of such distributions.

Form 5498G
Payments of Qualified Birth and Adoption Distributions are reported in Boxes 14a and 14b on Form 5498. The repayments should not be reported in Box 2 as a rollover.

Form 1099-R
Qualified Birth or Adoption Distributions are reported in Box 7 of Form 1099-R with a Code 1 – Early distribution, no known exception, Code J – Early distribution from a Roth IRA, or Code S – Early distribution from a SIMPLE IRA in the first 2 years, no known exception. The IRA owner is responsible for claiming the penalty exception for the Qualified Birth or Adoption on their taxes.

590-B
On February 19, 2020, the IRS posted an updated version of Publication 590-B that covers distributions from Traditional and Roth IRAs including the rules for required minimum distributions and distributions to beneficiaries. Updates in the ‘What’s New for 2020’ include the change in required beginning date for IRA

Compliance Systems • 1575 Arboretum Drive SE, Suite 406 • Grand Rapids, MI 49546
TEL 800.968.8522 • www.compliancesystems.com

owners who were born after June 30, 1949 and a notice that there are new distribution rules for designated beneficiaries of IRAs whose owner passes away in 2020 or years later.

590-A
On February 24, 2020, the IRS posted an updated version of the Publication 590-A, which covers contributions to Traditional and Roth IRAs including the rules for contribution eligibility. Highlights from the 'What's New for 2020' includes the repeal of the maximum age for making Traditional IRA contributions. It's also noted that the age for making required minimum distributions was changed to 72 from 70 ½.

Compliance Systems continues to monitor for guidance on these changes and will be making changes to our solution as necessary. Because of the scope of the SECURE Act, financial institutions will likely have to send amendments to existing plan owners and start using the updated documents when creating new plans. As we have in the past, Compliance Systems will provide surgical amendments for financial institutions to send to their IRA plan owners.

Update on the California Consumer Privacy Act

In June 2018, the State of California passed the California Consumer Privacy Act (CCPA), a sweeping privacy regulation intended to protect the personal information of its residents. The CCPA regulates how the personal information of California residents is maintained and seeks to allow residents more control over their information.

The CCPA became effective January 1, 2020. However, enforcement of the CCPA will generally not occur until July 1, 2020. Amendments to the legislation have been adopted such that enforcement of key parts of the CCPA in certain scenarios will not occur until a later date. For example, the enforcement date for many of the requirements of the CCPA with regard to the information of certain consumers captured as part of a business to business transaction has been extended until January 1, 2021. This extension is important because unlike many other privacy requirements, the definition of a "consumer" who is provided protection under the CCPA includes all natural persons who are California residents, regardless of whether those natural persons are engaged in business or consumer activities. While this extension is helpful for many businesses, the extension is not generally applicable to all requirements in all commercial-purpose transactions. Instead, it only applies to consumer information from a business to business transaction where the consumer whose information is collected is an employee, owner, director, officer, or contractor of a business customer, which may or may not cover all persons in a commercial transaction. While the extension applies to some CCPA requirements (e.g., the requirement to provide a notice at collection), it does not cover all CCPA requirements, such as the right to opt-out, non-discrimination, and data breach provisions.

In addition to its sweeping coverage of the personal information of any California resident, the CCPA requires compliance by a broad spectrum of businesses. Businesses do not need to be located in California to be subject to this Act. Rather, the Act is generally applicable to those doing business in California that collect or have direction over consumer personal information and meet certain revenue or activity thresholds. Among those thresholds, the business must have gross revenues in excess of $25,000,000; or buy, receive, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or derive 50% or more of its annual revenue from selling consumers' personal information. Because of this, compliance may be required for many businesses throughout the country. We recommend that our clients each engage in an assessment of their California activities to determine whether the CCPA may be applicable to them.

While application of the CCPA is wide-ranging, compliance with the law is not yet settled and therefore building CCPA compliance programs has been challenging. The initial proposed regulations were published on October 11, 2019. However, amendments to those regulations were made on February 10th and March 11th, and as of the time of this article the regulations are not yet final. Each round of amendments has brought with it significant changes to the compliance requirements and therefore the final content cannot yet be predicted.

It appears that an initial framework for notice structure is settled, although the content of the notices and required processes continues to evolve. The CCPA regulations break out the various requirements in the statute as separate notices: Notice at Collection of Personal Information, Notice of Right to Opt-Out of Sale of Personal Information, Notice of Financial Incentive, and a Privacy Policy, which includes the Right to Know, Right to Request Deletion, Right to Opt-Out, and Right to Non-Discrimination (among other items).

Compliance Systems currently supports a CCPA-compliant Privacy Policy as part of its general Privacy Policy and will be making modifications to that document based on the final form of the regulations. Compliance Systems is also developing a standalone Notice at Collection, which may be provided by businesses in accordance with their CCPA compliance policies. We continue to monitor the developments in CCPA compliance as well as the similar statutes pending in other states across the country. Compliance Systems will continue to provide updates regarding the developments on privacy laws as they occur and will be providing additional resources to assist our clients with their compliance strategies.

Abusive Acts and Practices: CFPB's Policy Statement

Since the inception of the Consumer Financial Protection Bureau (CFPB), one of the common concerns voiced by players in the financial industry relates to the Bureau's broad discretion in applying the Dodd-Frank's abusiveness standard when reviewing the actions of covered financial institutions and persons. This concern stems from the opinion that Dodd-Frank's "abusiveness standard" lacks clear definition, which makes it challenging for many financial services providers to understand what is needed to satisfy the standard. In a recent effort to further define Dodd-Frank's abusiveness standard, the Bureau has issued a "Statement of Policy Regarding Prohibition on Abusive Acts or Practices."

What is a Policy Statement?
Before summarizing the content of the Bureau's statement, it's important to understand how policy statements are defined. Policy statements are guidance documents issued by a regulatory agency with the purpose of explaining how a final rule applies to the public. Unlike substantive rules, policy statements are not subject to public comment and cannot create new requirements or amend legal standards. Instead, policy statements are interpretive rules that seek to explain how the agency interprets an existing rule, how the rule may be applied, and the steps people may take to comply with the rule.

What is an Unfair, Deceptive, Abusive act or Practice (UDAAP)?
Dodd-Frank section 1031(d) sets forth the statutory standard for what constitutes an abusive act or practice and states:

"Bureau shall have no authority under this section to declare an act or practice abusive in connection with the provision of a consumer financial product or service, unless the act or practice (1) Materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of—(A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.

Although section 1031(d) establishes a framework through which an abusive act or practice is identified, the Bureau recognizes that abusiveness standard is only defined in general terms, and the Act does not elaborate on what constitutes an abusive act or practice. This lack of specificity combined with limited historical context related to abusive acts and practices as defined under section 2031(d) has led the Bureau to conclude that the current abusiveness standard is uncertain, that this uncertainty is not beneficial, that financial service providers face significant challenges when attempting to comply with the abusiveness standard, and that consumers are

likely losing “the benefits of improved products or services and lower prices.”

What does the CFPB policy statement provide?
In the Policy Statement, the Bureau articulates its intended approach when employing the abusiveness standard in supervision and enforcement actions. Per the Policy Statement, the Bureau intends to focus on three different areas:

1. *Abusive Acts or Practices – Harms vs. Benefits*

Recognizing that Dodd-Frank charged it to implement and enforce consumer protection laws for purposes of ensuring that “consumers have access to markets for… financial product and services,” and that those markets are “fair, transparent, and competitive,” the Bureau clarified its intent to focus on actions and conduct, the results of which it concludes harms consumers more than it benefits consumers. While the Bureau did not enumerate the types of actions or conduct deemed more harmful than beneficial, it provided a basis upon which a financial service provider can examine its conduct.

2. *What Act or Practices Violate the Abusiveness Standard*

Generally, the Bureau will refrain from challenging conduct as abusive if the facts (all or nearly all) of the abusiveness charge are the same as an alleged unfair or deceptive act. The Bureau will, however, continue to pursue standalone abusive conduct and intends to “plead such claims in a manner designated to demonstrate clearly the nexus between the cited facts and the… legal analysis.” The Bureau also intends to provide more clarity related to the factual basis for citing certain conduct as abusive, planning to describe the factual basis for abusiveness citations in greater detail in future editions of Supervisory Highlights.

3. *Monetary Damages and Good-Faith Efforts to Comply*

Recognizing that uncertainty related to what is or is not a violation of abusiveness standard may deter certain lenders from offering products or services that would otherwise benefit consumers, the Bureau clarified its general intent to not seek monetary damages in situations in which the actor made a good-faith effort to comply with the abusiveness standard. While it will continue to seek legal or equitable remedies for redress identifiable consumer injury, the Bureau does “not intend to seek civil penalties or disgorgement” for those who made good-faith efforts to comply.

Conclusion
While the policy statement may not provide all the texture desired by financial service providers, it certainly appears to be a step in the direction of clarity. Based on the Policy Statement, what we witness in the coming months, whether through the Bureau’s supervisor and enforcement actions or the information it provides through its Supervisory Highlights, it appears that more clarity is yet to come.

Link to Privacy Statement

What Role Does Compliance Play in Your Bank’s Digital Strategy?

A Greek philosopher once said that no one can ever step into the same river twice. If Greek philosophers were defining how the financial industry works today, they might say that no bank can ever step into the same technology stream twice. Twenty-first century innovations, evolving standards, and new business requirements keep the landscape fluid, and that’s without factoring in the perpetual challenge of regulatory changes. As you evaluate your institution’s digital strategic plan, you should consider opportunities to address both technology and compliance transformations with the same solution.

Your bank’s investment in compliance technology sets the stage for how you operate today and in the future. Are you working with a compliance partner who delivers the same solution that they did two, five, or even ten years ago? Consider the turnover in consumer electronics in that same period. Your compliance partner’s

Compliance Systems • 1575 Arboretum Drive SE, Suite 406 • Grand Rapids, MI 49546
TEL 800.968.8522 • www.compliancesystems.com

reaction time becomes your bank's reaction time. If your compliance partner is not integrated with cloud-based systems, does not offer solutions tailored for online banking, and does not support an integrated data workflow, then it isn't likely they can position you for the next technology development, either. If your institution is looking to change core providers, platform providers, or extend your solution through APIs, the limitations of a dated compliance solution will only have a multiplying effect on the time and costs associated with these projects.

Your compliance partner must safeguard data integrity. Digital data is the backbone of your business. You need a compliance partner who doesn't store PII or otherwise expose your bank to the risks associated with data breaches. Your compliance partner's data management solution needs to offer secured access tiers while supporting a single system of record.

The best compliance partners know that service is a two-sided coin. Your compliance partner must understand your business challenges and offer a service model that connects your staff with legal and technology expertise to address their implementation questions. Leading compliance partners also understand that service isn't just about having seasoned professionals ready to answer questions. It's about offering a solution that's easy to set up in the first place, along with training resources that reach all your teams across your business footprint. It's about offering a solution designed to deliver an efficient user experience—and minimizes the need to make a support call.

You need a compliance partner who values and respects your bank's content control. Configurability should be part of your compliance partner's culture. Your products and terms belong to you. It's the responsibility of your compliance partner to make sure that your transactions support the configurability you need to service your customers. You can't afford a compliance technology approach that either restricts your ability to innovate your deposit products and commercial and consumer loans or permanently chains you to standard products or language or workarounds to get the output necessary to serve the customer. When configurability is an essential component of your solution, you can be confident that your bank can competitively adapt today and in the future.

Your compliance partner's ability to meet your needs depends on an active feedback loop. True partners never approach their relationship with your bank as a once-and-done conversation. They understand that the demands on your business will evolve and that their solution needs to meet you where you are and where you will be. If they're invested in their own success, then they cultivate opportunities to learn how they can grow their solution to meet your challenges.
Your compliance solution shouldn't be a siloed add-on to your digital operations. The right compliance partner aligns their solution with your overall objectives and helps extend your business reach. Make sure that your compliance technology investment positions your bank for long-term ROI.

Community Lounge Update

We have expanded our Community Lounge to include two new helpful forums for your institution. The Regulatory & Industry Updates forum is dedicated to content regarding proposed and current regulatory changes and related actions and updates impacting users of deposit, TFA, consumer, commercial, and mortgage products. The Update Spotlights forum contains content regarding changes in our solution that may have broader impacts on our documents, Simplicity Configuration, and Simplicity Runtime.

Click the green subscribe button to be email notified when we post a new topic. Subscribe

Link to the Community Lounge is here: https://community.compliancesystems.com/

Compliance Systems • 1575 Arboretum Drive SE, Suite 406 • Grand Rapids, MI 49546
TEL 800.968.8522 • www.compliancesystems.com

Additional Products Spotlight

Compliance Systems strives to offer your institution the products and services that help you maintain your competitive edge in a rapidly evolving business environment. We have now expanded Simplicity Configuration to provide you with access to some of those offerings. When you log into Simplicity Configuration, you'll see a new tab named Additional Products. Today, this is where you'll find convenient access to our new marketing portal containing IRA and HSA lobby brochures, statement stuffers, and SECURE Act content as well as links to more information regarding additional IRA and HSA services that can help your institution manage these challenging products.

In addition, our Deposit Business Continuity feature in Simplicity Configuration has been updated as well. Instead of managing an inventory of printed forms, you will now be able to satisfy your business continuity objectives with fillable PDF forms. For those of you who have not licensed Business Continuity, this product allows you to access to your entire Deposit document library, which then you can export as fillable PDFs in case of an internet outage or interruption in platform connectivity.

This update has been provided to your platform provider. You should have access to these new features in the coming weeks.

For any questions, please contact our Support Team at support@compliancesystems.com.

If you would like to purchase any of the additional products, please contact sales@compliancesystems.com.

Compliance Systems • 1575 Arboretum Drive SE, Suite 406 • Grand Rapids, MI 49546
TEL 800.968.8522 • www.compliancesystems.com