International Bancshares
Corporation

April 6, 2021

Via email submission:
regs.comments@federalreserve.gov
comments@fdic.gov

Federal Reserve Board of Governors
Ms. Ann E. Misback, Secretary
Attn: Docket No. R-1736, RIN 7100-AG06
20th Street and Constitution Avenue NW
Washington, DC 20551

Federal Deposit Insurance Corporation
Mr. James P. Sheesley, Assistant Secretary
Attn: Comments, RIN 3064--AF59
550 17th Street NW
Washington, DC 20429

Re: Comments on Notice of Proposed Rulemaking Regarding Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Federal Reserve Board Docket No. R-1736, RIN 7100-AG06; Federal Deposit Insurance Corporation RIN 3064-AF59)

Dear Sir or Madam:

The following comments are submitted by International Bancshares Corporation ("IBC"), a publicly-traded, multi-bank financial holding company headquartered in Laredo, Texas. IBC maintains 187 facilities and 284 ATMs, serving 88 communities in Texas and Oklahoma through five separately state-chartered banks ("IBC Banks") ranging in size from approximately $400 million to $10 billion, with consolidated assets totaling approximately $14 billion. IBC is one of the largest independent commercial bank holding companies headquartered in Texas.

This letter responds to the notice of proposed rulemaking ("Notice") by the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve Board ("FRB"), and the Federal Deposit Insurance Corporation ("FDIC," collectively the "Agencies") related to certain changes to regulations governing a banking organization's notice to its federal regulator of any "computer-security incident."

P.O. DRAWER 1359, LAREDO, TEXAS 78042-1359 (956) 722-7611

Under the proposed rule, a banking organization would be required to provide its primary federal regulator "with prompt notification of any 'computer-security incident' that rises to the level of a 'notification incident'...as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred." (Notice at 2299.) Moreover, the rule would require a bank service provider to notify at least two individuals at the affected banking organization immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided for four or more hours. (Notice at 2299.)

The proposed rule broadly defines "bank service providers" as a "bank service company or other person providing services to a banking organization that is subject to the Bank Service Company Act ("BSCA")." Bank services that are subject to the BSCA include check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, data processing, back office services, activities related to credit extensions and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution, as well as components that underlie these activities. (Notice at 2302.)

Under the proposed rule, a "computer-security incident" is an "occurrence that results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." (Notice at 2300.) The proposed rule defines "notification incident" as a "significant computer-security incident that could jeopardize the viability of the operations of an individual banking organization, result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector." (Notice at 2300.) Specifically, a "notification incident" is a "computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair:

1. The ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

2. Any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or

3. Those operations of a banking organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States." (Notice at 2302.)

As an initial matter, IBC wishes to be very clear: the types of "notification incidents" which the proposed rule covers are almost all *crimes* and, as such, banking organizations and their service providers are already highly incentivized (and in almost every case, required) to provide timely (sometimes immediate) notice to a regulator and/or law enforcement.

The proposed rule is generally duplicative of other existing requirements, as noted by the Agencies (Notice at 2301), and will only impose a completely unrealistic timetable onto those already existing requirements.

To the extent the proposed rule is meant to make cyber breach notification processes more uniform and consistent, as stated by the Agencies (Notice at 2304), it is difficult to see what progress the proposed rule is making towards that goal. The rule requires no specific information, follow up, or formal contact/notice method. While providing universal definitions is helpful, the proposed rule leaves much to be desired in the areas of uniformity and consistency. How is the rule substantively different than other existing obligations on banking organizations to identify and investigate cybercrime and report such incidents to law enforcement and regulators? The proposed rule's definition of "notification incident" is functionally inclusive of events and incidents that banking organizations are already incredibly motivated and required to report.

The Notice invites input on several general and specific issues related to the proposed computer-security incident notification rule. IBC has provided general comments and comments to the Agencies' specific requests for input below.

1. How should the definition of "computer-security incident" be modified, if at all? For example, should it include only occurrences that result in *actual* harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits? Should it include only occurrences that constitute an *actual* violation of security policies, security procedures, or acceptable use policies?

> **IBC Comment:** The proposed definition of "computer-security incident" is too broad and speculative to result in the benefits sought by the Agencies. The definition as written would force internal compliance and security teams to engage in hypotheticals and, in order to ensure compliance, they will necessarily need to err on the side of inclusion and reporting, resulting in the unnecessary reporting of all potential vulnerabilities, low risk of harm events and other specters of imagined harm. Therefore, instead of achieving the stated goals of the rulemaking, programs designed to meet the proposed rule would be based upon mitigating the liability of non-compliance through over-identification and over-reporting, trigging inefficiencies that will cascade down the notification stream and reduce the ability of internal compliance and security teams to properly identify, mitigate and report truly harmful events.
>
> Regarding the proposed "computer-security incident" definition in 12 C.F.R. 225.301 and 304.22, the inclusion of "potential harm" makes this definition too broad. For example, one reasonable interpretation of this definition would include any newly discovered vulnerabilities (such as the recent Microsoft Exchange Server vulnerability) that should not fit the definition of an "incident" without a corresponding act or tangible event that results in actual harm.

The definition also faces a similar scope problem with the inclusion of "imminent threat of violation." Any disgruntled employee with appropriate access could be considered an "imminent threat" to an organization's acceptable use policy. Overly broad and speculative definitions of triggering events result in an over-abundance of reportable events and a mass-triggering of compliance workflows that can cripple a business's internal IT, data privacy and security, and compliance teams. This can result in (i) inefficiencies resulting from overreporting to the required entities, starting a domino effect of triggered compliance workflows resulting in down-stream overreporting; (ii) decreasing the likelihood that events with actual harm are quickly identified, mitigated and timely reported; and (iii) decreasing the ability of the Agencies to identify important and relevant trends and to coordinate assistance to the affected entities because the Agencies will need to process a massive amount of reported incidents, most of which will be mere vulnerabilities or low/no risk of harm events.

Therefore, IBC recommends the terms "potential harm" and "imminent threat of violation" should be removed from the definition of "computer-security incident." An alternative approach to address this overly-broad definition would be to strike "an occurrence that-" and replace it with a more specific triggering verb, such as "an act."

2. How should the definition of "notification incident" be modified, if at all? For example, instead of "computer-security incident," should the definition of "notification incident" refer to other NIST terms and definitions, or another recognized source of terms and definitions? Should the standard for materially disrupt, degrade, or impair be altered to reduce potential redundancy between the terms or to consider different types of impact on the banking organization? Should the definition not include language that is consistent with the "core business line" and "critical operation" definitions included in the resolution-planning rule? Should those elements of the definition only apply to banking organizations that have resolution planning requirements?

IBC Comment: Similar to the issues with the definition of "computer-security incident," the speculative nature of the definition ("believes in good faith could materially disrupt, degrade, or impair....") would force internal compliance and security teams to engage in hypotheticals and, in order to ensure compliance, they will necessarily need to err on the side of inclusion and reporting, resulting in the unnecessary reporting of all potential vulnerabilities, low risk of harm events and other phantoms of imagined harm. Therefore, instead of achieving the stated goals of the rulemaking, programs designed to meet the proposed rule would be based upon mitigating the liability of non-compliance through over-identification and over-reporting, decreasing the ability of the Agencies to identify important and relevant trends and to coordinate assistance to the affected entities because the Agencies will need to process a massive amount of reported incidents, most of which will be mere vulnerabilities or low/no risk of harm events.

Therefore, IBC recommends the definition of "Notification incident" be backwards-looking, and be altered to read "is a computer-security incident that a banking organization believes in good faith has materially disrupt**ed**, degrad**ed**, or impair**ed**...."

3. How should the 36 hour timeframe for notification be modified, if at all, and why? Should it be made shorter or longer? Should it start at a different time? Should the timeframe be modified for certain types of notification incidents or banking organizations (for example, should banks with total assets of less than $10 billion have a different timeframe)?

IBC Comment: The 36 hour notification timeline should adjusted to five business days, or, at the very least, 72 hours. Notably, IBC believes the proposed timeframe is still shorter than under any existing law or regulation. For example, both the European Union's General Data Protection Regulation and the New York Department of Financial Services' Cybersecurity Regulation require notification of certain incidents within 72 hours.

While there are incidents where the impact is known immediately, in a ransomware event the victim's systems are generally taken offline (or degraded) fairly quickly and remain so for a period of time. At that point, the victim's 36 hour notification requirement would start to toll. In a massive ransomware incident, at 36 hours, the victim needs to be solely focused on recovery and remediation. If the victim needs technical assistance or guidance, then it can contact its Agency regulator within that window. None of the stated goals of the rulemaking require such a strict timeline for reporting. Moreover, in the event of a ransomware (or other ongoing catastrophic event), it is almost certainly the case that law enforcement will be notified and brought in to assist almost immediately once the issue is identified. Further, requiring Agency notice within such a short time period is either redundant or harmful as efforts are diverted from actual investigation and remediation.

IBC also supports the Agencies' providing alternative timeline requirements for banking organizations with total assets under a certain amount. IBC supports a longer notification timeline for banking organizations with less than $20 billion in total assets. This change would acknowledge the additional burden on banking organizations and the differing risks and needs of such organizations. Large institutions may face more risk of cyberattack, given their generally broader online footprint and product and service offerings, as well as the potentially larger criminal pay out for a successful cyberattack. Many small and mid-sized banking institutions do not have as robust online banking product and service offerings, and may face less risk of cyberattack given their potentially lower profiles. It follows that such banking organizations should have more flexibility in notifying their regulators of such notification incidents.

4. Is the proposed requirement that banking organizations and bank service providers notify the appropriate party when they "believe in good faith" that they are experiencing or have experienced a notification incident or computer-security incident, as applicable, sufficiently clear such that banking organizations and bank service providers understand when they should provide notice? How should the "believes in good faith" standard be modified, if at all? For example, should the standard be "reasonably believes" for either banking organizations or bank service providers?

> **IBC Comment:** To experienced bankers and legal practitioners, the "good faith" standard is generally workable to identify situations where they should provide notice. Unlike many other industries, banking organizations have been subject to data regulation for decades and many will have the know-how to make such a determination. However, it is naïve to assume that all organizations subject to the proposed rule will have the necessary institutional knowledge sufficient for compliance, resulting in overreporting or underreporting. Therefore, IBC believes the Agencies should provide practical guidance (such as detailed case studies) sufficient to inform internal compliance and security teams regarding how they should make this good faith determination.

5. How should notification by banking organizations under the proposed rule be provided to the agencies? Should the agencies adopt a process for joint notification to the agencies in cases where multiple affiliates of a banking organization have notification requirements to different agencies? If so, how should joint notification be done and why? Should the agencies adopt centralized points of contact to receive notifications or should notifications be provided to regional offices (such as Federal Reserve Banks) or banking organization-specific supervisory teams?

> **IBC Comment:** IBC believes the Agencies should adopt a process for joint, uniform notice. In almost every case, multiple Agencies require notification. For example, a bank branch that experiences a notification incident will be required to notify the OCC or FDIC, in addition to the bank's holding company notifying the FRB. The Agencies should provide a joint telephone number, email address, and/or web portal to allow banking organizations to provide the required notice. As the notice does not require any specific information, the joint contact points could be as simple as a banking organization "pressing 1" on an automatic telephone menu to report a notification incident, with the onus on the Agency to follow up with the banking organization's listed point of contact for such notice. The proposed rule is already going to require time and energy that could otherwise be devoted to addressing the notification incident. The Agencies should do everything possible to streamline the notification process.

7. What other types of entities regulated by the agencies should be added to the rule as "banking organizations" that would be subject to the rule? Why?

IBC Comment: To the extent the Agencies, specifically the OCC, charter or otherwise oversee non-depository institutions or financial services fintechs, such entities should be included as "banking organizations" to the extent they would not otherwise be covered as "bank service providers."

As has been the clear recent trend, such fintechs and non-traditional depository institutions are being given the keys to the U.S. financial system with almost none of the attendant regulatory and legal burdens that come with such a privilege. Most disappointingly, the Agencies are continuing to pile regulatory burdens onto insured depository institutions while letting fintechs and other new players enter the industry unimpeded by such concerns. As drafted, it is unclear whether an institution chartered under a limited use OCC charter would be considered a "banking organization." While many financial services fintechs would be considered "bank service providers" under the proposed rule, certain of those entities should likely be considered "banking organizations" unto themselves. The Agencies should ensure that chartered depository institutions are not further undermined and disadvantaged by suffocating regulations that do not also apply to other industry participants, such as fintechs.

9. Do existing contracts between banking organizations and bank service providers already have provisions that would allow banking organizations to meet the proposed notification incident requirements?

> **IBC Comment:** Due to the increase in banking and finance technology, in addition to consumer data and privacy laws, depository institutions generally require their banking service providers to commit contractually to stringent data and cyber security terms, including unauthorized access and breach notification requirements. However, these terms are typically structured based on definitions, triggers, and timelines that differ from the Agencies' proposal. As discussed herein, such terms are generally based on actual acts and occurrences, and not "potential harm" and "imminent threat." The terms do not require hypothetical evaluations and analyses. Rather the focus is on the actual occurrence of a harmful event or action. Moreover, it is not uncommon for the notification timeline to be based around identification and good faith belief instead of a set timeline. For example, notification of a cyber-security incident may be required "within a commercially reasonable time following identification" based on the severity of such event (e.g. if no consumer data was compromised and the attack merely slowed down services, notice may be required within 5 business days).
>
> While IBC believes the vast majority of bank service provider contracts are subject to cyber-security notification requirements (as applicable), that is not to say the proposed rule would be easily implemented as the Agencies' proposed terms are not industry standard. Banking organizations would almost certainly be required to execute additional riders or terms with their bank services providers in order to ensure compliance with the new rule.

10. Does the definition of "bank service provider" in the proposed rule appropriately capture the services about which banking organizations should be informed in the event of disruptions? Should all the services included in the Bank Service Company Act be included for purposes of banking organizations receiving notice of disruptions from their bank service providers? If not, which services should require a bank service provider to notify its affected banking organization customers when those services are disrupted, and why?

Should the requirement only attach to a subset of services provided to banking organizations under the BSCA or should it only attach to certain bank service providers, such as those that are examined by the federal banking agencies?

IBC Comment: IBC believes the proposed rule should apply to any banking service that includes the transmittal or handling of personally identifiable consumer information or data or that is fundamental to a banking organization's ability to carry out and provide its banking operations. However, given the Agencies' position that "[r]egulators would enforce the bank service provider notification requirement directly against bank service providers and would not cite a banking organization because a service provider fails to comply with the service provider notification requirement," IBC is supportive of using BSCA-covered services in the interest of clarity and uniformity. (Notice at 2303.)

11. Should the proposed rule for bank service providers require bank service providers to notify all banking organization customers or only those affected by a computer-security incident under the proposed rule?

> **IBC Comment:** The rule should not mandate notification of all banking organization customers. When dealing with a serious breach or ransomware event, internal compliance and security teams must focus on immediate containment, remediation and interaction with those entities/individuals who are at risk of harm as a result of the event. Mandating notification to unaffected entities/individuals will require internal compliance and security teams, which will be already stressed to the breaking point, to devote extremely limited time and resources to address non-essential questions, complaints and inquiries from low or no-risk entities/individuals. They will likely be unable to do so efficiently or satisfactorily during a time of crisis, and their efforts to do so will reduce their effectiveness in handling the effects of the event. Further, according to the 2020 Cost of a Data Breach Report by the Ponemon Institute and published by IBM Security (available at https://www.ibm.com/security/data-breach), loss of business remains the highest cost of a data breach. Forcing notification to unaffected entities/individuals will increase this loss of business unnecessarily, especially if the bank service provider is still devoting its resources to addressing the event and affected banking organization customers. Undoubtably, there are advantages to notifying all banking organization customers and the bank service provider may choose to do so for their own benefit as well as for the benefit of their customers, but they should not be forced to do so.

12. Within what timeframe should bank service providers provide notification to banking organizations? Is immediate notification after experiencing a disruption in services provided to affected banking organization customers and to report to those organizations reasonable? If not, what is the appropriate amount of time for a bank service provider to determine it has experienced a material disruption in service that impacts its banking organization customers, and why?

IBC Comment: Bank service provider notification timelines should be bifurcated: one immediate notice timeline if the incident affects the security of the banking organization's systems and a second, longer time period for disruption. In practice, notification regarding disruption of service is often governed contractually between the parties, so the timelines presented in the rule should be drafted as a maximum limit and should certainly be longer than 36 hours.

13. The agencies understand that many existing contracts between banking organizations and bank service providers contain notification provisions regarding material incidents and that, generally, bank service providers use automated systems to notify banking organizations of service disruptions. The agencies are seeking information on how bank service providers currently notify banking organizations of service disruptions under existing contracts between bank service providers and banking organizations. Do those contracts contemplate the provision of notice to at least two individuals at an affected banking organization? Is the method of notice specified in existing contracts (for example, email, telephone, etc.) sufficient to allow bank service providers to provide notice of computer-security incidents to at least two individuals at affected banking organizations? If not, how best could the requirement for bank service providers to notify at least two individuals at affected banking organizations be achieved most efficiently and cost effectively for both parties?

IBC Comment: IBC believes that the current contractual provisions with bank service providers commonly provide specific notice methods and generally provide notice to two or more banking organization employees. For example, such notification is typically required via email or other electronic means which is generally available to multiple banking organization employees, such as an email listserv. IBC recommends the Agencies make clear that notification through a medium or channel that is accessed by and available to multiple banking organization employees would meet this requirement.

15. The agencies invite comments on specific examples of computer-security incidents that should, or should not, constitute notification incidents.

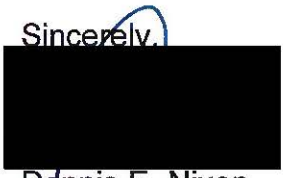
IBC Comment: IBC believes that the detection of vulnerabilities should not be a notification incident. A banking organization that has not been harmed or suffered damages from a technological vulnerability that is identified and remediated should not be required to report such event as a "notification incident." Such identification and remediation is simply a fundamental piece of a banking organization's continued obligation to monitor, evaluate, secure, and improve its technological capabilities and offerings. This carve out would be self-effecting if, as discussed herein, the Agencies revise the proposed definition to only apply to incidents that have "disrupt**ed**, degrad**ed**, or impair**ed**" the covered banking services and operations.

16. The agencies invite comments on the methodology used to estimate the number of notification incidents per year that would need to be reported under the proposed rule.

IBC Comment: While IBC is not in a position to estimate the number of notification events across all banking organizations and bank service providers, it is telling that the Agencies relied on existing supervisory data and SARs involving cyber events in order to estimate the annual number of notification incidents under the proposed rule. The Agencies *already have the notice and information access they are seeking* through this proposed rule. As discussed throughout, banking organizations are already generally required to provide such notice and information to both their regulators and law enforcement. The proposed rule is duplicative and would appear to add little value to the already existing notice framework for cyber-security events.

Thank you for the opportunity to share IBC's views.

Sincerely,



Dennis E. Nixon
President and CEO