Aldrich & Bonnefin, PLC

Counsel to Bankers' Compliance Group® presents

2023 Bank Counsel Seminar

FedNow & Cybersecurity

Speaker:

Keith R. Forrester, Esq.

ALDRICH & BONNEFIN

Professional Law Corporation

THE FEDNOW SERVICE

ALDRICH & BONNEFIN
Professional Law Corporation

Real-Time Payments

- Payments that are initiated by either businesses or consumers and are then settled nearly instantaneously
- One real benefit to RTP networks is the ability to provide around the clock access, 365 days a year, including weekends and holidays

ALDRICH & BONNEFIN
Professional Law Corporation

Real-Time Payments

- The most prominent example of an RTP network in the U.S. is The Clearing House's RTP network
- The FedNow Service is the Federal Reserve Banks' version of RTP expected to launch in 2023

ALDRICH & BONNEFIN
Professional Law Corporation

Regulation J Amendments

- Subpart B of Regulation J provides rules that govern funds transfers through the Reserve Banks' Fedwire Funds Service
- The Board amended Regulation J by establishing a new Subpart C that deals with the FedNow Service
- Many of the concepts embodied in Subpart C are similar to those currently in Subpart B which deals with Fedwire

ALDRICH & BONNEFIN
Professional Law Corporation

FedNow Launch Services

- Core clearing and settlement capabilities to support a range of transaction types and use cases
- Use of the widely accepted ISO® 20022 standard and other industry best practices to support interoperability
- Features that are intended to support flexible adoption, including support for the use of service providers and correspondents and an option to enroll as a “receive-only” participant

ALDRICH & BONNEFIN
Professional Law Corporation

FedNow Launch Services

- Value-added features including request-for-payment capability and tools to support participants in their handling of payment inquiries, reconcilements and certain exceptions
- Features to enhance experience for financial institutions by broadcasting participant availability to support the following
  - The transition to 24x7x365 operations
  - A user interface to support data needs
  - The ability to have access to balance information on weekends

ALDRICH & BONNEFIN
Professional Law Corporation

FedNow Launch Services

- Features to support payment integrity and data security and tools to help financial institutions combat fraud
  - Such as a transaction value limit and reporting features
- A liquidity-management tool that will allow participants and others to transfer funds to each other to support the liquidity needs of instant payments

ALDRICH & BONNEFIN
Professional Law Corporation

Payment Flow

- Step 1
  - A sender initiates a payment by sending a payment message to its financial institution through an end-user interface outside the FedNow Service
  - The sender's financial institution is responsible for screening the payment according to its internal processes and requirements

ALDRICH & BONNEFIN
Professional Law Corporation

Payment Flow

- Step 2
  - The sender's financial institution submits a payment message to the FedNow Service
- Step 3
  - The FedNow Service validates the payment message, for example, by verifying that the message meets message format specifications

ALDRICH & BONNEFIN
Professional Law Corporation

Payment Flow

- Step 4
  - The FedNow Service sends the contents of the payment message to the receiver's financial institution to seek confirmation that the receiver's financial institution intends to accept the payment message
  - At this point, the receiver's financial institution will have the opportunity to confirm or deny that it maintains the specified account

ALDRICH & BONNEFIN
Professional Law Corporation

Payment Flow

- Step 5
  - The receiver's financial institution sends a positive response to the FedNow Service, confirming that it intends to accept the payment message
  - Steps 4 and 5 are intended to reduce the number of misdirected payments and resulting exception cases that can occur in high-volume systems

ALDRICH & BONNEFIN
Professional Law Corporation

Payment Flow

- Step 6
  - The FedNow Service debits and credits the designated master accounts of the sender's and receiver's financial institutions (or their correspondent financial institutions), respectively

ALDRICH & BONNEFIN
Professional Law Corporation

Payment Flow

- Step 7
  - The FedNow Service sends a payment message forward to the receiver's financial institution with an advice of credit
  - In parallel, sends an acknowledgement to the sender's financial institution, notifying it that settlement is complete

ALDRICH & BONNEFIN
Professional Law Corporation

Payment Flow

- Step 8
  - The receiver's financial institution credits the receiver's account
  - The receiver's financial institution must agree to make funds available to the receiver almost immediately after Step 7
  - This crediting to the receiver's account as well as the debiting of the sender's account by their respective financial institutions happens outside the FedNow Service

ALDRICH & BONNEFIN
Professional Law Corporation

FedNow To Adopt ISO 20022

- The federal reserve banks published the ISO 20022 messaging specifications that define the message flows and formats the FedNow Service uses
- The FedNow Service uses a variety of ISO message types including:
  - For customer credit transfers
  - Requests for payment and interbank liquidity transfers
  - The FedNow system and account reporting messages

ALDRICH & BONNEFIN
Professional Law Corporation

FedNow To Adopt ISO 20022

- On October 6, 2021, the Board published an announcement in the Federal Register that the federal reserve banks will adopt the ISO 20022 message format for the Fedwire Funds Service as well

ALDRICH & BONNEFIN
Professional Law Corporation

Interaction With EFTA

- Unlike the Fedwire Funds Service, which is designed to serve primarily as a large-value funds transfer system between institutional users, the FedNow Service is designed to also accommodate consumer users

ALDRICH & BONNEFIN
Professional Law Corporation

Interaction With EFTA

- Subpart C provides that UCC Article 4A applies to all funds transfers over the FedNow Service
  - This includes a transfer from a consumer originator or a transfer to a consumer beneficiary that is carried out through the FedNow Service
- By its terms, UCC Article 4A would not apply to a funds transfer any part of which is governed by the EFTA

ALDRICH & BONNEFIN
Professional Law Corporation

Interaction With EFTA

- To deal with this discrepancy, Section 210.40 provides that all transfers over the FedNow Service are covered by Subpart C (which incorporates UCC Article 4A by reference)
- And this is intended to include those transfers any portion of which is governed by the EFTA

ALDRICH & BONNEFIN
Professional Law Corporation

Interaction With EFTA

- Therefore, in the event a transfer over the FedNow Service meets the definition of “electronic fund transfer” under the EFTA, Subpart C provides that it would still apply to the transfer
- However, the EFTA would prevail to the extent of any inconsistency

ALDRICH & BONNEFIN
Professional Law Corporation

Example

- The commentary to Section 210.40 provides an example
- A funds transfer may be initiated from a consumer's account at a financial institution
- The institution will then execute that payment order by sending a conforming payment order to a Reserve Bank through the FedNow Service

ALDRICH & BONNEFIN
Professional Law Corporation

Example (cont)

- The consumer subsequently provides timely notice to its financial institution that the electronic funds transfer was unauthorized
- The institution would be required to comply with the error resolution requirements of the EFTA (and Regulation E)

ALDRICH & BONNEFIN
Professional Law Corporation

Example (cont)

- Basically, the EFTA/Regulation E error resolution requirements will apply
- This is the case even if the institution does not have a right to receive a refund or reverse the payment order sent through the FedNow Service

ALDRICH & BONNEFIN
Professional Law Corporation

GLBA BREACH NOTIFICATION REQUIREMENTS

ALDRICH & BONNEFIN
Professional Law Corporation

Notice Obligation

- Financial institutions have an affirmative duty to protect customer information against unauthorized access or use
- Notifying customers of a data breach is a key part of that duty

ALDRICH & BONNEFIN
Professional Law Corporation

What is a "Data Breach"?

- Under GLBA:
  - "Unauthorized access to or use of customer information
  - That could result in substantial harm or inconvenience to a customer"
- CA defines "*breach of the security of the system*" to mean:
  - Unauthorized acquisition of computerized data
  - That compromises the security, confidentiality, or integrity of "*personal information*" maintained by the business

ALDRICH & BONNEFIN
Professional Law Corporation

Definitions from Security Guidelines

- "Customer"
  - A consumer who has a "continuing relationship" with a financial institution
- "Consumer"
  - An individual who obtains a financial product or service for primarily personal, family or household purposes

ALDRICH & BONNEFIN
Professional Law Corporation

"Nonpublic Personal Information"

- Personally identifiable financial information, and
- Any list, description or other grouping of consumers
- That is derived using any personally identifiable financial information that is not publicly available

ALDRICH & BONNEFIN
Professional Law Corporation

“Sensitive Customer Information”

- One from Column 1 and one from Column 2:

Column 1	Column 2
(1) Name;	(1) Social security number;
(2) Address; or	(2) Driver’s license number;
(3) Telephone number;	(3) Account number;
	(4) Credit or debit card number; or
	(5) A personal identification number or password that would permit access to the customer’s account.

ALDRICH & BONNEFIN
Professional Law Corporation

“Sensitive Customer Information”

- The term also includes any combination of components of customer information that would allow someone to log onto or access a customer’s account
- Refer to Exhibit E for chart of notice requirements

ALDRICH & BONNEFIN
Professional Law Corporation

When Should Notice Be Made?

- It is very difficult to determine when customer notification of a security breach is warranted
- When unauthorized access to customer information is discovered, institution must conduct a reasonable investigation
  - Substantial harm or inconvenience to a customer is most likely to result from improper access to “sensitive customer information”
  - Sensitive customer information is most likely to be misused by identity thieves

ALDRICH & BONNEFIN
Professional Law Corporation

Notify Affected Customers

- Determine based on the investigation that misuse of sensitive customer information has occurred or it is reasonably possible
- Affected customers should be notified as soon as possible

ALDRICH & BONNEFIN
Professional Law Corporation

Banking Agencies New Breach Notification Rule

- On November 23, 2021 OCC, FRB and FDIC issued a final rule to add new breach notification requirements on financial institutions and certain service providers
  - Institutions are required to timely notify their primary federal regulator after the occurrence of an event that rises to the level of a “notification incident”
  - Certain types of bank service providers are required to notify a designated point of contact at the affected institution if the service provider is subject to certain types of breaches

ALDRICH & BONNEFIN
Professional Law Corporation

Notice to a Primary Federal Regulator

- Notice to a primary federal regulator is required for any “computer-security incident” that rises to the level of a “notification incident”

ALDRICH & BONNEFIN
Professional Law Corporation

Notice to a Primary Federal Regulator

- A “computer security incident”
  - Results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits
- A “notification incident”
  - Computer-security incident that has materially disrupted or degraded certain components of a banking organization’s business operations
- Scope of “business operations”
  - The institution’s ability to function
  - The institution’s material business lines
  - Material profit or revenue loss

ALDRICH & BONNEFIN
Professional Law Corporation

Delivery of Notice

- Notify primary federal regulator as soon as possible
  - In no case later than 36 hours after determine notification incident has occurred
- Notify the agency supervisory office or designated point of contact via email, telephone or similar method
- Agencies anticipate that banking organizations will share general information about what it knows at the time of an incident

ALDRICH & BONNEFIN
Professional Law Corporation

Notification by Bank Service Providers

- Covered service providers are required to notify the affected banking organization if the service provider suffers a notification incident that impacts the services provided to the affected banking organization
  - "Bank service providers" means a bank service company or other person that performs "covered services"
  - "Covered services" refer to any of a banking organization's vendors or service providers subject to the Bank Service Company Act

ALDRICH & BONNEFIN
Professional Law Corporation

Computer Security Incidents

- If the covered service provider has experienced a computer-security incident that has materially disrupted or degraded for four or more hours
- Notice not required if the incident pertains to scheduled maintenance, testing or a software update previously communicated

ALDRICH & BONNEFIN
Professional Law Corporation

Notice Requirement

- Requires service provider to notify the banking organization as soon as possible after determining incident has occurred
- Notice must be to either a bank designated point of contact or two executives at the affected banking organization
- Final Rule does not impose any guidelines on the information or content that a covered service provider must include in its notice

ALDRICH & BONNEFIN
Professional Law Corporation

NCUA New Breach Notification Rules

- On March 1, 2023, the NCUA published a Final Rule
- Requires FICUs to report to the NCUA as soon as possible following a “reportable cyber incident”
- But no later than 72 hours after it has experienced a reportable cyber incident

ALDRICH & BONNEFIN
Professional Law Corporation

CALIFORNIA DATA BREACH LAW

ALDRICH & BONNEFIN
Professional Law Corporation

Customer Notification

- California Civil Code Section 1798.82
  - Imposes customer notification requirements
  - Notice required when a breach of the security of customer data has occurred

ALDRICH & BONNEFIN
Professional Law Corporation

Scope of Coverage

- Covers any person or business that conducts business in California if the person owns, licenses or maintains computerized data that includes "personal information"
- Requires disclosure of breach of the security of the data to any resident of California whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person

ALDRICH & BONNEFIN
Professional Law Corporation

Breach

- Breach of the security of the system
- Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of “personal information” maintained by the business

ALDRICH & BONNEFIN
Professional Law Corporation

Personal Information

- Column 1 and one from Column 2

Column 1	Column 2
First name or first initial AND Last name	(1) Social security number; (2) Driver's license number or California identification card number; (3) Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account; (4) Medical information; or (5) Health insurance information

ALDRICH & BONNEFIN
Professional Law Corporation

Special Rule for Online Account Access

- “Personal information” also includes user name or email address
- In combination with a password or security question and answer that would permit access to an online account

ALDRICH & BONNEFIN
Professional Law Corporation

Form of Notice

- Written notice can be provided to affected individuals whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person
- Electronic Notice
  - Can be provided so long as the business complies with the E-SIGN Act
  - This means that prior disclosure and consent must be obtained from the individual before the notice may be given solely in electronic form

ALDRICH & BONNEFIN
Professional Law Corporation

Online Accounts

- If breach involves a user name or email address, in combination with a password or security question and answer
- Notice can be provided electronically or in any other form

ALDRICH & BONNEFIN
Professional Law Corporation

Online Accounts

- Must direct the person to:
  - Change password and security question or answer promptly, or
  - Take other steps appropriate to protect the online account and all other online accounts
    - For which the person uses the same user name or email address and password or security question and answer

ALDRICH & BONNEFIN
Professional Law Corporation

Model Notice Format

- Must be written in plain language
- Must be titled, “Notice of Data Breach”
- Must be organized using the following headings:
  - “What Information Was Involved”
  - What We Are Doing”
  - “What You Can Do”
  - “For More Information”

ALDRICH & BONNEFIN
Professional Law Corporation

Model Notice Format

- The notice must be in a font no smaller than 10-point type, and
- In a format designed to call attention to the nature and significance of the information

ALDRICH & BONNEFIN
Professional Law Corporation

Notice Must Include the Following

- A general description of the breach incident
- Toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed:
  - Social security number
  - Driver's license number, or
  - California identification card number

ALDRICH & BONNEFIN
Professional Law Corporation

Notice Must Include the Following

- If the business providing the notice was the source of the breach:
  - An offer to provide appropriate identity theft prevention and mitigation services
    - At no cost to the affected person
    - For not less than 12 months
  - The offer is to be given to any person whose social security number or driver's license or California identification card number was compromised

ALDRICH & BONNEFIN
Professional Law Corporation

Notice to Attorney General

- A business that is required to issue a security breach notice to more than 500 California residents as a result of a single breach of its security system, must notify the CA AG
- The institution should electronically submit a single sample copy of that security breach notice, excluding any personally identifiable information

ALDRICH & BONNEFIN
Professional Law Corporation

QUESTIONS?

ALDRICH & BONNEFIN
Professional Law Corporation

Speaker Contact Information

Keith R. Forrester, Esq.
Principal
Aldrich & Bonnefin, PLC
(949) 474-1944
KForrester@ABLawyers.com