NACHA AND TOKENIZATION

Accurate Efficient Data Protection

June 2021

ALPINE
Security Consulting

EXECUTIVE SUMMARY

Changes in how to protect what data occur more frequently today than ever before. Simplifying the approach to data protection and ensuring the ability to keep up with all of these changes, while still maintaining access to the usefulness of this data, is a growing challenge for most organizations.

This paper will address this simplification while reviewing the new Nacha data security rule as an example of how leveraging the right approach to tokenization can be used to meet these moving targets. Only a well-designed data protection approach can properly address the many data security regulations and still provide the benefits of being able to access this protected data in a way that enables an organization to continuously utilize the value of the data.

The Nacha rule will be briefly reviewed so that you can identify how this mandate applies to your organization and evaluate the challenge and risks your organization is facing. Once the challenge is understood, tokenization and encryption will be reviewed as example of one of the best approaches to solve this challenge. Key functions to look for in encryption and tokenization solutions will be covered.

Comforte's SecurDPS data security platform will then be reviewed to assess how the data protection approach they offer meets the Nacha Rule specifically as well as meets the larger data security challenges from multiple regulations and still offers the utility of using the data for business needs.

NACHA RULE OVERVIEW

The Nacha Operating Rules and Guidelines are the foundation for ACH payments. The Operating Rules are the legal framework for the ACH Network and explain the rights and obligations for Network participants. The Guidelines expand on the Rules and provide best practices for Network participants and additional guidance for recently implemented Rules. This paper is focused on the Security portions of the Rules and Guidelines, and specifically on the new Data Security requirements that are going to be enforced for Network participants.

WHAT IS THE RULE?

Simply put, the rule is about protecting the account number in an ACH transaction.
The most important aspect is that the account data needs to be rendered unreadable when storing it electronically. The supplement states this as well:

> **The rule aligns with existing language contained in PCI requirements, thus industry participants are expected to be reasonably familiar with the manner and intent of the requirement.**

Note that this rule does not apply to the storage of paper authorizations.

For the full details you can refer to the Rules, Article One, Section 1.6 and the Supplement for Data Security Requirements. It should also be noted that Section 1.7 covers protection of account data when it is transmitted and has always been a requirement. These requirements go hand in hand and should be considered together in order to meet them properly.

WHO CARES?

Anyone who collects account numbers for an ACH transaction. Financial institutions who are already covered by existing Federal Financial Institutions Examination Council (FFIEC) or similar data security requirements and regulations already care because those regulations have required them to do this protection for account numbers. This rule has no new impact on them since they already were required to do this protection.

Large non-financial Originators, Third-Party Service Providers and Third-Party Senders are not subject to FFIEC and therefore this Rule is intended to enforce these data protection requirements on these entities.

NACHA RULE OVERVIEW

WHY AND WHEN DO I CARE?

If your organization wants to continue to take ACH transactions, you need to meet the requirements for this Rule as soon as possible to avoid potential fines and penalties. There are very few business justifications, if any, to wait to implement or have a well-defined plan to implement these protections. The Rule was introduced in November of 2018 as a supplement. The first phase of the rule was for ACH Originators and Third-Parties of 6-million ACH payments annually in the calendar year 2019 to fully comply to the Rule by June 30, 2020. This has been extended to **June 30, 2021**. The second phase is for those with an ACH volume of 2 million during the calendar year of 2020 to be fully compliant with the rule by **June 30, 2022**.

With these dates, if you don't have a plan to meet the requirements in place, you are at a high risk to fail to meet the requirements on time, regardless of how many transactions you authorize.

HOW DO I FOLLOW THE RULE?

The best way to protect account data when stored electronically is with encryption and/or tokenization.

Nacha stays neutral as to the specific methods to render account data unreadable, but the most common industry standards are to encrypt or tokenize this sensitive data. Since Nacha refers specifically to PCI, the PCI DSS resources here can be leveraged and this resource can be leveraged to assist with industry standard mapping between PCI and the National Institute of Standards and Technology (NIST).

Fully and properly protecting account data for ACH is much the same as protecting other sensitive data from an IT and security perspective. Meeting the security requirements of Nacha, PCI or NIST, and still maintaining functionality of existing business practices and the value the data has for daily operations, is a delicate and challenging balance.

KEYS TO DATA PROTECTION

There are many aspects to consider when protecting sensitive data. The following are the top things you need to consider when protecting account data for ACH processing using tokenization or encryption technologies.

REGULATIONS AND REQUIREMENTS

Because Nacha is not technically specific, it is easier to confirm how PCI applies to ACH account data rather than leverage what Nacha provides technically. If you have protected your ACH account data the same way as your Cardholder Data (CHD) is protected under the PCI DSS, then you are on solid ground. If you have not done this yet, you can leverage PCI's resources and/or a seasoned security expert to ensure your approach to encryption or tokenization will meet the requirements. The primary goal here is to ensure that the details of your encryption or tokenization solution will fully comply with ACH along with any other requirements you must follow. This means you must know what data you have, such as ACH account data, and where that data resides and travels.

FLEXIBILITY

Securing the data without disrupting existing business practices more than necessary can be a huge challenge. When encrypting or tokenizing, you should look for options to maintain the data structure you already have while still ensuring the security of the data.

ACCESS TO VALUE

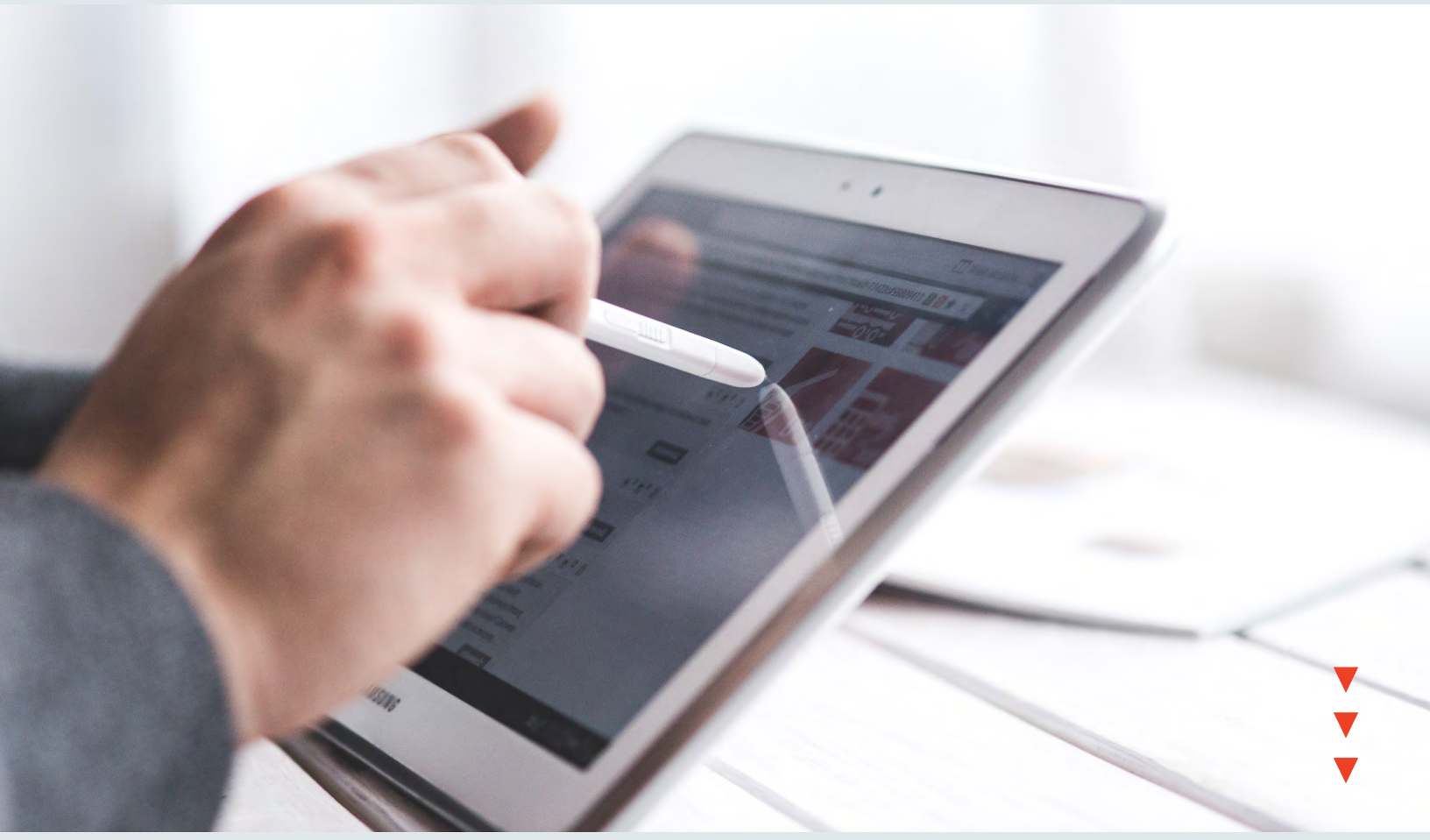
Protecting the data with encryption or tokenization can often lose the ability to leverage the data the way an organization has done for years. Finding a solution that allows for the business intelligence that comes from access to data as well as securing the data is a top priority for most organizations. Finding the right solution that can do this can often lead to more business value from the data than in the past as well.

KEYS TO DATA PROTECTION

SPEED TO IMPLEMENT

Even if you can find a solution for your data protection needs that is fully secure, meets all the requirements you need, allows flexibility, and maintains the value of the data, it is all for nothing if it takes too long to implement and causes massive disruptions to your organization's day-to-day operations. When looking at a data protection solution, you must understand the effort and time it takes to put the solution in place and run at full speed. The ideal solution will be one that can be implemented quickly and still offer a data-centric approach to securing your sensitive data.

Combining a full understanding of an organization's data environment with these considerations provides an excellent start when looking for an encryption and tokenization approach to make the best decision possible for any organizations business needs and data security goals.



COMFORTE'S SECURDPS

With so many options to protect your sensitive data, it's critical to understand the above factors to evaluate any solution. Here we will review how SecurDPS from comforte addresses these data protection challenges in a comprehensive way for any organization facing multiple requirements, including ACH, PCI, NIST and many more.

SecurDPS offers an enterprise tokenization and encryption solution through an integration framework that is flexible and scalable. Here are the key functions that can be observed in SecurDPS:

- **The ability to meet or exceed the data protection requirements from virtually any standard or regulation including Nacha, PCI DSS, NIST, GDPR, HIPAA/HITECH, FedRamp, CMMC, SOX and many more.**
- **The functionality to find, track, classify and inventory sensitive data from any of the above standards or regulations.**
- **Support for multiple deployment options from Hybrid to Multi-Cloud to Native Cloud.**
- **The flexibility to be integrated easily into any environment with little to no code changes, minimizing disruption to daily business operations.**
- **The scalability of tokenization methodologies including vaultless technology and encryption based tokenization or Format Preserving Encryption (FPE).**
- **The security to maintain the value of the protected data, and even increase the value of the sensitive data to business intelligence needs.**
- **A data-centric approach to identifying, classifying and securing all sensitive data across complex environments.**
- **The ability to implement strong data protection with all of the above benefits in timelines as short as weeks instead of months or years.**

SecureDPS offers a unique approach to data protection that can be leveraged by any organization needing to meet the new Nacha Rule around data security in a way that moves beyond simply meeting a set of checkboxes and offers additional data protection and business value.

CONCLUSION

Nacha's new data security Rule is another in a long list of examples of how the regulations and standards continue to evolve and apply to every organization. Understanding the specifics of Nacha, or any data protection requirement, is just the first step to ensuring an organization is prepared to properly protect the sensitive data they handle. Failing to do this well and on time can lead to many negative consequences including fines, loss of business, brand damage and more. The ability to leverage the best data protection methods quickly and effectively can avoid the negative aspects as well as turn into business efficiencies and functionalities that can accelerate profits and expand opportunities.

The Nacha data security Rule may not apply today, but today is the time to address the concern. Comforte's SecurDPS is at the top of the list of data security options to consider to address Nacha's data security Rule, as well as address the multitude of other data security challenges an organization faces today. Used well, SecurDPS can move an organization from a reactive approach to security and compliance concerns into a proactive business mode that will enable long term success.

ABOUT ALPINE: WWW.ALPINECONSULTS.COM

Alpine was founded to fulfill a passion to help businesses, and the people that work in them, overcome today's cybersecurity challenges and succeed in new ways by leveraging the untapped value that an innovative approach to security can provide. With a background of over 20 years in technology, security and compliance, Alpine's skill set can help virtually any business learn how to leverage innovative security technologies with the result of translating security investments into tangible business value.

ABOUT COMFORTE: WWW.COMFORTE.COM

Comforte helps companies all over the world to protect hundreds of millions of payment transactions, healthcare records, insurance records, and more, reliably running in business-critical environments. With more than 20 years of experience in data protection on truly mission-critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: data.

ABOUT THE AUTHOR: DAN FRITSCHE, CISSP

Dan Fritsche, CISSP, is Founder of Alpine Security Consulting. Dan's specialty is in security innovation, helping companies of all kinds turn security from a hurdle into a strategic investment that has a positive return on investment. Dan started out with a security focus for 10 years at IBM, actively supporting penetration testing, vulnerability scanning, application security and business intelligence across multiple security disciplines. This led to 10 years at Coalfire helping hundreds of companies improve their security posture in application security, encryption, tokenization, and many other security specialties. Dan went on to help Global Payments drive the value and involvement of innovative security approaches as early into applications lifecycles as possible. Dan is a former QSA, PA-QSA, P2PE QSA and P2PE PA-QSA of 5-10 years each.

CREATED BY: HAMMER & CHISEL DESIGN COMPANY, LLC | www.hammerandchiseldesign.com HCD005-21