Payment Security Best Practices in Enterprise Financial Operations

What keeps finance executives up at night? The same thing that keeps the rest of us awake — security breaches. As the business world becomes more global and digital, the need for payment security has grown with it. A successful breach can result in the loss of millions of dollars, as well as damage a company's reputation.

As financial technology, or fintech, continues to advance, there are new ways for businesses to accept payments. While the use of credit and debit cards is still the most common form of payment for both online and in-person transactions, the implementation of new fintech services is on the rise.

Card payments are an increasingly popular payment option for many in the US. The number of cards used - Visa, MasterCard, American Express, and Discover - reached 694 million in 2019, according to CardData. With this impressive volume comes a 5.2% year-on-year growth forecast that will see 768 052 576 cards available for use by the end of 2021!

The payments industry is growing and shifting at a rapid pace, becoming more complex as new technologies and diverse payment methods emerge. In addition, the regulatory environment is often complex and ever-changing, requiring payment service providers to ensure their processes are secure and compliant with current rules and regulations.

There are several strategies and best practices that companies can utilize to ensure the security of their payments, as this post will outline.

What Are Enterprise Payment Solutions and Their Benefits?

Enterprise payment solutions are a comprehensive payment platform that balances anonymity and transparency. The engine process payments through the appropriate channels and provide tracking and reporting to both the financial institution and the customer.

For firms processing transactions at a much larger scale with many different locations (nationally and internationally), it can be challenging to keep track of which payments are authorized and which aren't. A streamlined process will allow for not only a broader range of payment solutions but also accommodates for different types of payments.

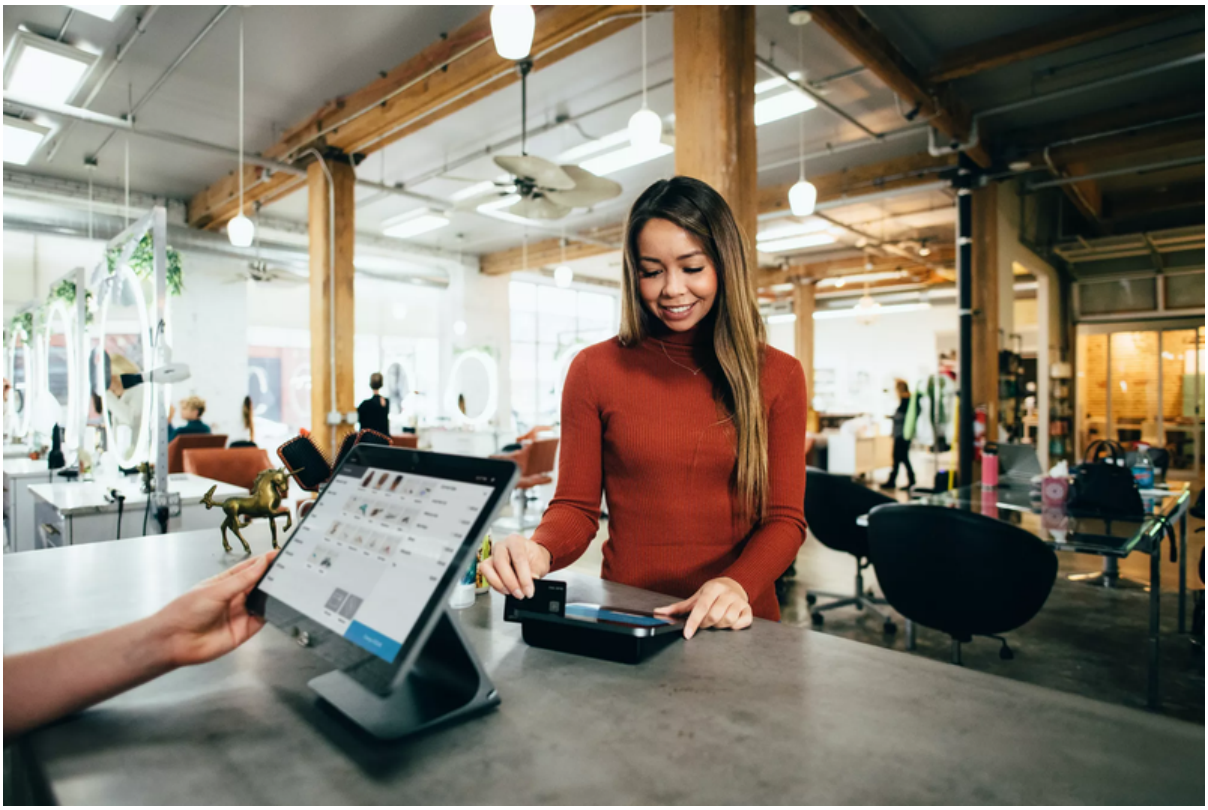
Enterprise payment solutions work as fast, easy, and secure payment hubs - they create a unified network of payments that simplify things for you. You can monitor and manage all different types of payments, such as ACH, wire, instant payments, and TCH real-time payments, across a single, easy-to-use interface, and process these varied transaction types much faster.

With firms already having complex financial systems, the last thing you need is more complexity in terms of financial management and operations. Utilizing APIs, Enterprise Payment Solutions work with your financial systems already in place and simply connect them, allowing them to 'speak the same language' and giving you a platform that facilitates easy tracking and reporting with all your transaction data in one place.

Being able to get an easy overview of all your payment data, you can begin to create a much better payment strategy that reflects the cost per payment and payment channel with greater accuracy. Enterprise Payment Solutions give you a much broader view of your existing payment ecosystem. With this smart and efficient technology, you are able to not only see the bigger picture, but also zoom in on details such as receivables and payables, available payment options and methods, vendors, card volumes, and payment processes.

Monitoring individual aspects of the digital payment journey gives you the clarity needed to create comprehensive and holistic reports that can generate more accurate predictions and can help refine your financial strategy. Perhaps the biggest benefit of Enterprise Payment Solutions is the robust security protocols allowing you to closely monitor what comes in and out of numerous accounts, where it originates, and who it comes from.

Payment Security Tips in the Enterprise Payment Space



There is, however, the very real possibility that companies can fall victim to security breaches. Credit cards, for example, have allowed faster payments but also bring with them the risk of sensitive data getting into the wrong hands. With credit cards, it is not only card data that is stored but also personal identity data. Securely managing this data is thus crucial.

Take Advantage of Security Technologies

Address Verification System (AVS) – The system cross checks the credit card holder's address information that is on file against the address provided by the individual making a

transaction. After deciding whether this info matches or not, the system signals the merchant, who can make a verification request to the bank if they aren't all that confident in the information they receive.

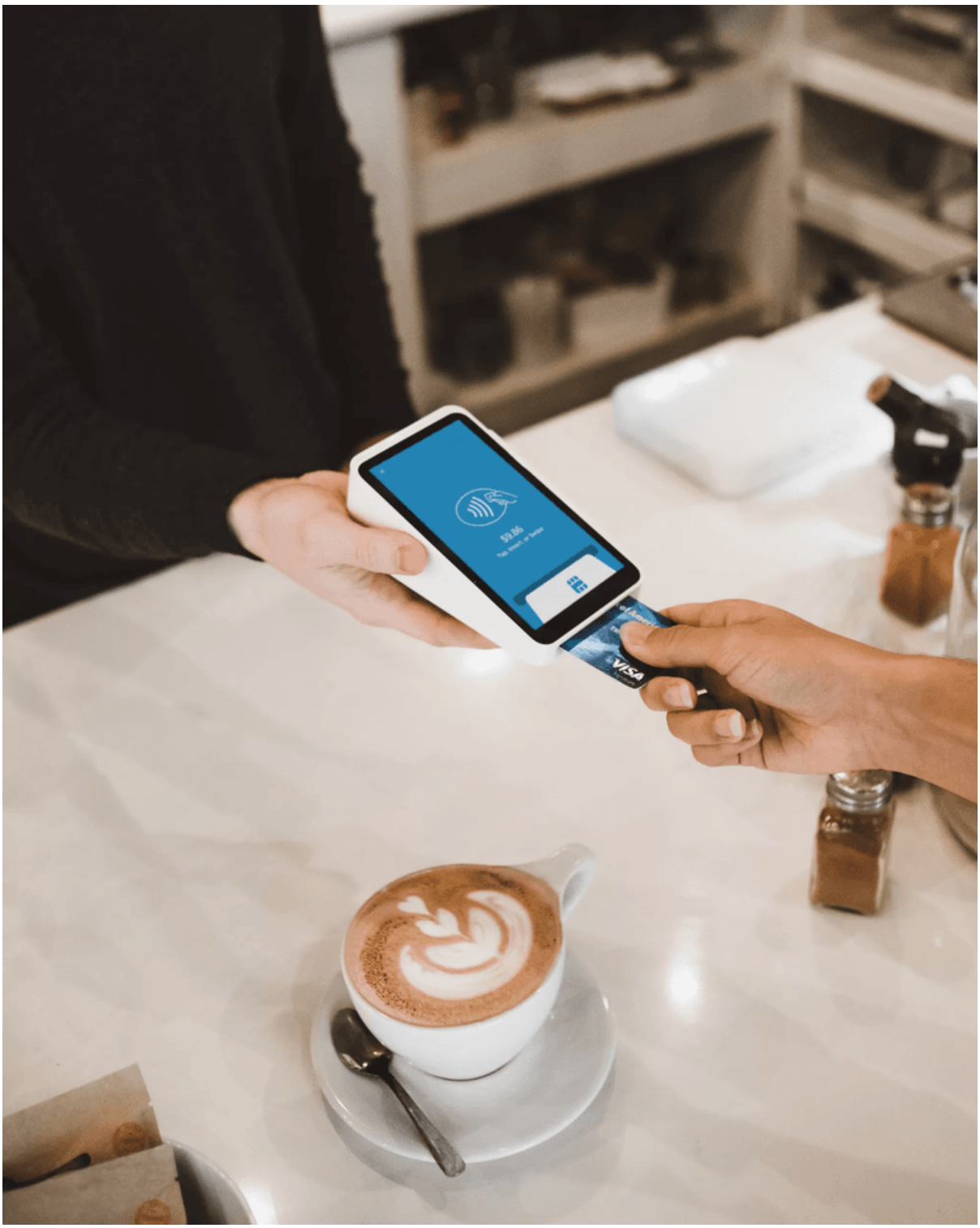
Upgrade to chip readers – Counterfeit cards are one of the most common types of fraud prevalent in US stores. It's an easy crime to commit and hard to solve. There is a good explanation for this: we're behind on implementing EMV technology (taken from a combination of the Europay, Mastercard, and Visa - the three credit card companies that developed the tech). The US has been slow to adopt chip readers, but it's high time they do.

Process online payments safely and securely – Even if you process payments online or over the phone, you can do this securely by look out for the following red flags before processing a payment:

- Orders that have several of the same items
- Orders involving "big-ticket" items, such as TVs.
- Multiple same-day purchases.
- Multiple purchases coming from the same IP address.
- "Rush" orders.
- Orders that have failed AVS (Address Verification Service) or CID (the three-digit value on the back of the card).
- International orders from countries that you usually don't have customers in.
- Orders that are shipped to a single address, but made on multiple cards or using multiple billing addresses.

Secure network access – Secure your network by limiting employee access to sensitive data, using updates to the latest versions of software, and increasing your cybersecurity efforts by using separate devices for your personal and business use. Roll out layered security measures like generating strong, complex passwords as well as two-factor authentication. System encryption can keep malicious third parties from getting their hands on your information.

Ensure PCI Compliance



PCI or Payment Card Industry compliance is a non-negotiable in terms of financial security in enterprise payments. PCI is all about strict data security standards and sets the bar for what customers should expect in terms of data protection from those handling their financial information.

While there's a range of actions an enterprise needs to take to meet compliance, they should focus on three important areas... And get a PCI consultant to guide them through the rest.

1. Collecting and transmitting credit card data securely.

2. Ensuring credit card data is stored safely and securely.

3. Annually proving that required security protocols are met.

Stamping out Human Error

The potential for human error always looms large and mistakes can put your entire system at risk. Here are four ways to mitigate this.

Installing anti-malware software. Employees connecting to your system can put you at risk by downloading malware onto their work devices (which most often happens without their knowledge), and consequently infecting your system. Anti-malware software installed on your systems can detect malware that may be present.

Limiting user credentials. This will help to ensure minimal damage even if hackers and cybercriminals gain access to a legitimate user's account.

Use logging mechanisms. You need to know who is accessing your system and what they've accessed. Monitoring user activity can help you find out what information they have access to and how to protect it.

Train your employees. Your workers should be thoroughly grounded in your enterprise's security processes, policies, and systems. That way, they can help keep systems secure and know what to do in the event of security breaches.

NatPay and ACH: The Smart, Secure Way To Handle Your Payments

National Payment Corporation (NatPay) has become the leading company to offer third-party processing of Direct Deposits for employee payroll, processing more than $115+ billion annually for 228,000+ ACH clients nationwide.

NatPay has been the pioneer in payroll distribution solutions since 1991, offering multiple levels of data encryption and file protection that is unmatched. In addition, NatPay is integrated with most accounting and payroll processing software. If not, no problem. We specialize in custom integrations.

The challenges of payment card processing can be circumvented entirely, and NatPay can help. As an industry leader in bulk payment processing services, we can help your enterprise sustain its success with our secure online systems. Book a demo today, and together, let's build a customized solution for your organization.