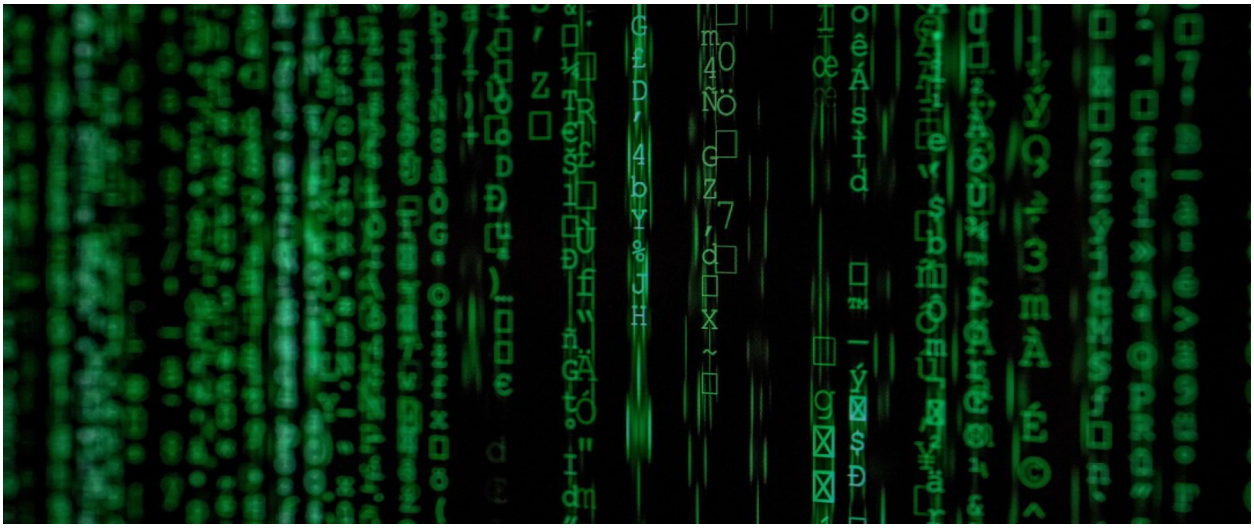
Developing Country Guide to Payment Fraud

Nick Brown wrote a series of posts on LinkedIn in 2018 relating to the scale of Payment Fraud, included below.

Part 1: Introduction to Payment Systems and Payment Fraud



Aug 2, 2018: Nick Brown, International Payment System Expert & Founder of Clear Purchase

This blog series is intended for anyone involved in offering financial services in developing countries, especially for those involving the poorest people in your country. This would likely include mobile money operators, micro-lenders, conventional banks, governments, micro-insurers, and others.

You are about to enter an incredibly exciting time in your country as all your financial systems start connecting together. The company you work for will grow massively just from taking this step as you start offering more services to your existing customers, and you also will gain more customers by offering those services. Every other company that connects benefits as well. Your whole country stands to benefit, including even the poorest people.

Warning: There are huge risks involved in connecting your system to others, which have the potential to be so damaging that your company may not survive. I am talking specifically about Payment Fraud, and the sheer scale of damage that can result from a major fraud attack.

This must not happen. What you are doing is too important to allow it to falter from lack of preparedness. As a technical expert in payment infrastructure, let me help you navigate through the turbulent waters that lie ahead.

The Payment Infrastructure Industry is Unique

Just over 30 years ago, I started working in the credit/debit card payment industry, and immediately discovered it was completely different in priorities and expectations from any other. One of the first projects I worked on was to make it possible for a bank to have two production data centers running in parallel I built the interface between their two data centers to duplicate transactions in real-time. That meant that, even if one data center was completely destroyed, the other would be able to run everything without interruption, and no transactions would be lost.

Having two parallel data centers in the ‘80s was staggeringly expensive to achieve, opening my eyes to the priorities they placed on this specific system of theirs.

My understanding of how unique payment processing is grew as I worked for different types of organizations in the payment industry, each with their own priorities and challenges -- big banks, major retailers, payment hubs, payment software vendors, even writing data security standards.

You have started along your own path into this industry, and I am sure you are excited with the potential that lies ahead -- just as I was many years ago. I now have the opportunity to share some of the knowledge I have gained over the last 30 years, assisting you as you follow your own path.

Why the focus on Payment Fraud?

There are many other challenges you will be dealing with as you grow your system and the services you offer, again many of them quite unique to this industry. For almost every challenge, the problems are well known, the costs involved in mitigating those problems are easily determined, and a logical decision can be made as to whether now is the time to address a particular problem.

The difference with Payment Fraud is by the time it happens it’s already too late.

It is impossible to build a perfect system, so there will always be ‘holes’ that allow for fraud. You will not know about a hole until your system is already in production, and the hole has been discovered and exploited. At that point you will not be able to shut down your system, as so many people will be relying on it. I know from experience that holes can seldom be fixed easily, and some cannot be fixed at all. You may be stuck with the fraud for a long time.

Fraud ***must*** be considered ***before*** a system goes live.

Payment Fraud is Huge

It took years for me to fully realize how huge and complex a problem payment fraud is.

There are two types of fraud, the first committed by individuals when they see an opportunity, for a few transactions here and there until it is stopped or they are caught. This is important and must be prevented and minimalized as soon as possible. However, unless it is ignored, this will not destroy your system and company.

The kind to be afraid of is that committed by the major international crime organizations that have been successfully attacking the well-protected systems here in the West, despite the vast amounts spent on protecting these systems. This is “big business” for them, with over $20 Billion of fraud every year, and growing.

When a new vulnerable target appears, they will pounce.

Interoperability Makes You a Target

For the criminal organizations, a closed system is of little interest: your systems are relatively easy to protect; a breach can generally be identified and fixed fairly quickly; and the fraud could probably be undone. They will ignore you.

Everything changes the moment your system is part of a network. An intrusion ***anywhere*** in the network will affect ***every*** system in the network, so you are now a huge target. With the whole network to look at, they will target the weakest link in the transaction chain. The attack will most

likely happen outside of your control, and yet you and your customers will suffer the consequences.

When they attack, it will not be a small number of transaction, it could easily be10 million transactions happening all at once. Are you prepared to handle that scale of fraud, with that many unhappy customers wondering where their money has gone? Who would compensate your customers? Would your company survive? This number is possible - when a big store chain here in the USA got their system hacked in 2013, 40 million credit/debit card numbers were stolen.

That's not all. It may be years for the hole to be fixed, as a fix would have to be found, and then would most likely require a coordinated upgrade by every single system in the network. The criminal organizations will happily continue taking advantage of the current hole in your network, while they are also looking for the next one, or creating it.

This is an easy prediction for me to make, as this is exactly what has been happening for decades with the credit/debit card systems here in the West.

Although this news might terrify you, and for good reason, be comforted by the knowledge that their current targets have been able to manage fraud sufficiently to remain extremely profitable, and will continue to do so into the future – as will you if you are sufficiently prepared.

Conclusion: Protect yourselves as you grow bigger

Congratulations! You have achieved what no one thought was possible - you are currently offering financial services to the poorest people in your country. You ignored conventional wisdom, and it worked!

You are about to take the next logical step, by connecting your system to other systems in order to process transactions between your account holders and theirs. This changes everything. You are now much more vulnerable to payment fraud, and much more enticing as a target.

If your systems are well protected, fraud will be minimized and manageable. You will then be able to forge ahead with confidence, offering more and more services to more and more customers. You and your company will benefit, just as your customers will benefit -- and so will your country!

Learn from my experience.

Part 2: The Real Costs of Payment Fraud

Aug 9, 2018: Nick Brown, International Payment System Expert & Founder of Clear Purchase

To my readers: If you thought the first blog in this series was worrisome, then this one might absolutely terrify you! Do not be too disheartened, however; once you understand what you are dealing with, payment fraud can become manageable. Notice that I have not said anywhere that it is possible to completely eliminate fraud -- only that fraud can be managed.

The real cost of payment fraud is not, however, the fraud itself. No, by far the biggest cost is fraud management. That's because you have to employ lots of people to answer unhappy customers' calls, and then involve all the other parties in the transaction chain to figure out the cause of the fraud and resolve it.

Interoperability Changes Everything

In my first blog, I described how becoming part of a network will result in your becoming more vulnerable to fraud, and much more of an enticing target to major criminal organizations.

Here is some more bad news – interoperability not only increases the amount of fraud, it also increases the cost of dealing with each instance of fraud.

So long as you have a closed system, where you control every part of a transaction from source to destination, your system is fairly defensible. There is likely to be minimal fraud, and the cost of managing and resolving any fraud that occurs is minimal as well.

But when you are part of a network, a transaction could involve 4 or 5 different companies. Resolving any fraud would involve employees from each company in the transaction chain talking to each other to determine what happened, discussing how to resolve it, and determining who is going to be left to deal with the fraud.

Your customers will soon be calling. But they will be calling you, expecting you to resolve the fraud, blaming you for the loss of money they entrusted with you for safekeeping -- regardless of whether the fraud happened on your system or elsewhere.

What happens when one of your customers is hit by fraud?

Imagine that a customer of yours is about to buy some groceries for her family; she suddenly realizes that her account is empty. As she studies the last few transactions, she notices one she doesn't recognize. Extremely unhappy and worried, she calls your support phone number, reasoning that she had, after all, entrusted you with her money… and now it's all gone.

What do you do? You will quickly see that her money was sent to a payment hub, and you know it will take time to resolve. Here's a big question – what do you tell your customer as she stands in a store, unable to pay for her purchase? Do you put funds into her account while this case is being resolved, or leave her with nothing?

Next, it's time to find out what actually happened. You will contact someone at the payment hub company who will contact the next company in the transaction chain, and so on, until the company that manages the receiver's account is reached. They will look into the transaction and their response will be passed back through each company, and finally to you.

If it is obvious that fraud took place, the situation can quickly be resolved.

However, what if there is a question as to whether the transaction was fraudulent or not? What if the receiver of those funds claims that the transaction was legitimate?

There are more possibilities. What if the receiver of the funds has disappeared? What if the receiver's bank doesn't respond to queries?

The fraud must now be resolved in some manner, and someone will take the hit. But everyone involved will argue that it is not their responsibility. It may take weeks before this is sorted out!

Your Cost: You will need to employ sufficient people to answer the phone calls of your customers, and to ultimately resolve the fraud.

The danger of a major fraud attack

And now for the worst news.

In the prior post, I talked about how fraud of opportunity by individuals is manageable. This is because each person only does a few transactions before it is noticed and stopped. Therefore, the total number of fraudulent transactions will be fairly consistent from month to month, so it is fairly easy to know how many employees will be involved to manage this type of fraud.

Now consider a major fraud attack that affects 1 million of your customers, most of whom call you the next day when they discover that their money is missing. Can you handle that many calls in one day?

Your business is based on your customers trusting you with their money. People understand that things can go wrong. However, if you want them to continue trusting you, then you must deal with problems promptly when they happen. The worst thing you can do to a customer is not answer the phone when she calls. Not only will she no longer trust you, she will tell everyone she knows what happened. Multiply this by a million customers, and you have a disaster!

Here is the big question: How many new employees must you hire to answer the phones, in order to cover a major fraud attack?

Managing Fraud: Follow the Procedures

Now it finally starts getting easier.

When you are part of a payment network, the only way for everything to work harmoniously is if everyone plays by the same rules, with clearly defined responsibilities for each member of the network.

The payment hub company must define responsibilities for each of the players in their network, and ensure that they are met. Your job is to understand the responsibilities you have been given, and fulfill them to the best of your abilities.

It is also the payment hub company's responsibility to provide the processes and procedures to follow for each type of occurrence that involves more than one player in their network, including all the various types of fraud.

The payment hub company is also responsible for assigning legal and financial liabilities to each player for each type of occurrence, and for the oversight of those liabilities.

Assess a Payment Hub Before You Connect

All the responsibility for a smooth-running payment network falls on the capabilities of the payment hub company.

A payment hub company must have a payment method (a transaction from end-to-end) that works for everyone involved. The easy part is when everything is working. The challenge is to plan for every type of occurrence of when things go wrong, whether it's system errors or intentional fraud.

My recommendation? Scrutinize the payment hub company and the payment method they are offering, in detail -- especially around the subjects of transaction integrity and security -- before you connect to their system. Do you understand all your responsibilities, whether operational, financial or legal? Do you, and the payment hub company, have a realistic assessment of the potential types and scale of fraud that might occur?

Ultimately, it comes down to whether you trust them or not. After all, think about it: Your survival is on the line!

Surely, this is an instance where it is far better to be safe than sorry.

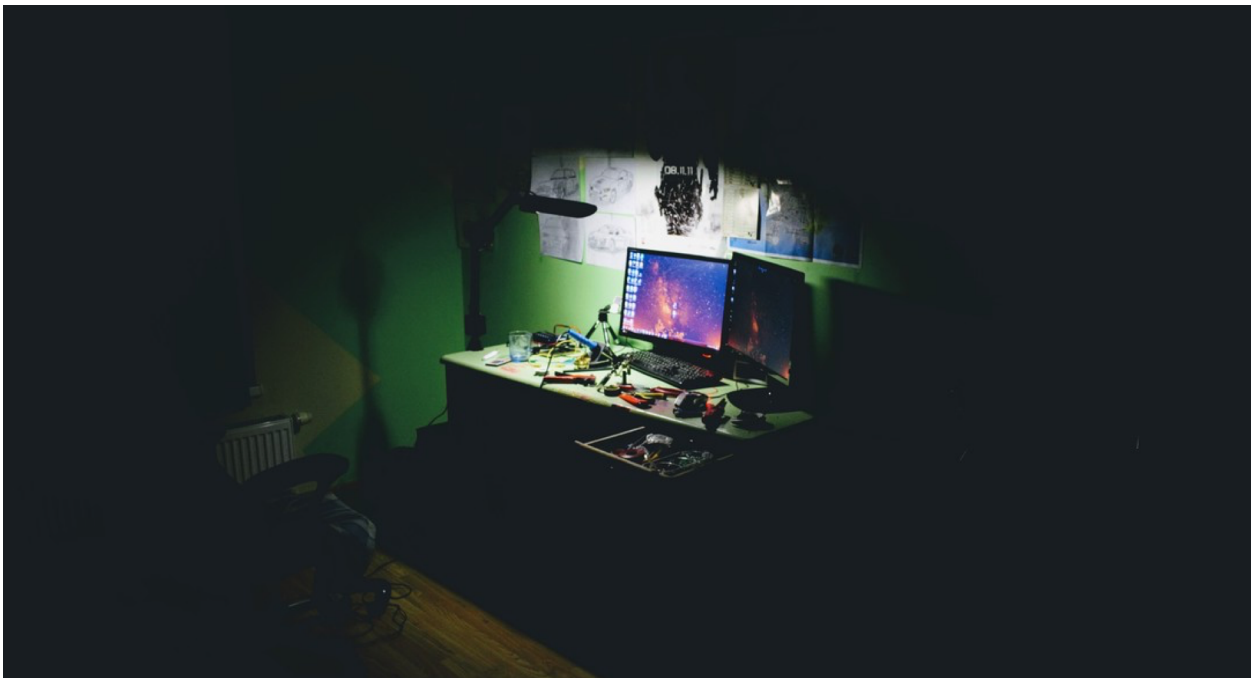
Summary

Now you have an idea of the real costs of payment fraud, and the devastating consequences of a major attack to you and your company.

The best way to minimize damage is to fully understand all the risks ***before*** you join a network. After something goes wrong, it is too late.

The type of payment method you adopt is vitally important: it determines the types of fraud that can happen – and the means to minimize the likelihood, as well as the damage, of fraud. We will start to examine these topics in the next blog in this series.

Part 3: The Vulnerabilities of "Pull" Payment Methods



Aug 23, 2018: Nick Brown, International Payment System Expert & Founder of Clear Purchase

Here in the West, almost all payment methods are described as "Pull," especially those that are high-volume and real-time, such as checks and credit/debit cards. Unfortunately, by their very nature, "Pull" payment methods have vulnerabilities that are relatively easy to exploit.

With the prevalence of cell phones, and the availability of Mobile Money, "Pull" methods are no longer inevitable.

I would highly recommend avoiding "Pull" payment methods, if possible.

What is a "Pull" payment method?

Very simply, a "Pull" payment method is where a receiver of funds "Pulls" funds from the sender's account, while in a "Push" payment method, a sender of funds "Pushes" funds from his account to the receiver.

All payment methods are either "Push," "Pull," or a combination of the two. As this blog relates to vulnerabilities to entire networks, it is appropriate to include under "Pull" those that are a combination of the two.

"Pull" payment systems/methods here in the West: credit cards, debit cards, ATM cards, checks, automatic bill payments, Apple Pay, PayPal, Western Union (credit/debit card), and so on. The central bank clearinghouse here in the USA (Automated Clearing House, or ACH) is both "Push" and "Pull."

"Push" payment systems/methods include store cards, wires (including SWIFT), Western Union (cash deposit), and, obviously, physical cash. Decentralized crypto currencies like Bitcoin also fall into this category, though they have other issues that I might discuss in the future.

How you can identify a "Pull" Payment System

Let's assume your company offers financial services to your customers. You are approached by an organization that wants to connect its system to yours, with the goal of facilitating financial transactions between your two systems. No doubt this scenario will sound ideal, with your company as well as your customers benefiting.

You will want to know whether this new system is a "Pull" system.

Ask yourself this question: Can a transaction be initiated at another organization, resulting in funds being "Pulled" from one of my customers' accounts? By the way, a continuation of an earlier transaction does not apply.

To put it another way: Is there ever a time when my system will receive a request message from another system, whereby my system is expected to withdraw funds from my customer's account and send it to the other company?

If the answer is yes, then it is a "Pull" system.

Why are "Pull" payment methods so vulnerable?

If you are connected to a "Pull" payment system, you will be obligated to trust every request message you receive, most initiated on systems run by companies you have never heard of. You will then have to send your customers' money to those companies.

No system is perfect, so it is inevitable that there will be errors, and also fraud. When this happens on a system other than yours, your customers' money could be at risk, and they will hold you accountable.

Once your system is connected to a "Pull" payment system, you are no longer in complete control of your own customers' accounts. This should scare you!

Lets play the "what If" game:

- What if the sender of a request entered the amount or the account number inaccurately?
- What if the sender of a request is not who they claim to be?
- What if your customer claims he didn't agree to a transaction?
- How much time does your customer have to notice a fraudulent transaction?

These questions are just the tip of the iceberg.

The "I didn't do that" transaction

Let's look at credit/debit card fraud, which exceeds $20 billion per year.

A customer looks at his account and sees a transaction he didn't make. He immediately calls his bank, informing them that he didn't make that specific transaction. This starts the process outlined in Blog #2.

The most likely outcome is that the customer will be credited the disputed amount, and either the merchant or the merchant's bank will cover the cost.

There are two steps in the process of committing credit/debit card fraud:

1. Card information is stolen. This generally happens at the weakest point in the network, namely, the merchant. For example, Target chain stores here in the USA had their system hacked in 2013, with information on 40 million credit/debit cards being stolen.

Notice it was the merchant system that was hacked, and yet it was the customer's bank account information that was stolen; therefore, it will be the customer and the customer's bank that will be most affected.

2. Fake transactions can be initiated at any merchant in the network. This step is incredibly easy to do online, the only question being whether the transactions are approved or declined. Even if only 5% are approved, we are still talking about 2 million customers hit from this one hack into Target's system in 2013.

This type of fraud would not happen with a 'Push" payment system.

Fraud Prevention Measures

Banks, card companies and merchants spend huge amounts of money on fraud prevention. The goal is to identify fraudulent transactions as they happen, and decline them.

Some experts have estimated the total cost of fraud prevention measures to be ½% of the value of all credit/debit card transactions.

Despite extensive fraud prevention measures, 8% of sales by online merchants are estimated to be fraudulent.

With all the fraud prevention measures, fraud management and the fraud itself, it is not surprising that credit card fees to the merchant are generally from 2% - 4%, with a minimum fee from 20¢ - 35¢. This minimum fee may not be that important here in the USA; however, for the poorest people in your country, that fee would be prohibitive.

Mobile Money is a "Push" Payment Method

A simple Mobile Money transfer is a "Push" payment:

> ***A customer uses his phone to directly instruct his Mobile Money Operator to send a specific amount of money from his account to a specific destination.***

Central to this statement is that the customer has continuous communication directly with his Mobile Money Operator.

As Mobile Money Operators provide more and more services to their customers, I highly recommend they ensure that every new service is based on the "Push" model.

The Bill & Melinda Gates Foundation Got it Right with Mojaloop

Mojaloop was developed by the Bill & Melinda Gates Foundation, in collaboration with several other excellent companies, for the specific purpose of accelerating the interoperability of financial systems in developing countries by building a standard communication module that will allow any financial system to talk to another financial system that also has Mojaloop.

Mojaloop is a "Push" payment module. Conventional wisdom would dictate that they would copy the credit card model; there was no real reason to question that. And yet they did.

The Bill & Melinda Gates Foundation deserves huge credit for having the insight to ask the right question, taking the time necessary to figure out all the advantages and disadvantages, and then making this decision. Next, they developed an impressive module -- without any certainty that it would be adopted. Kudos to the Bill & Melinda Gates Foundation!

For the record, our decision at Clear Purchase not to adopt Mojaloop was based on other considerations.

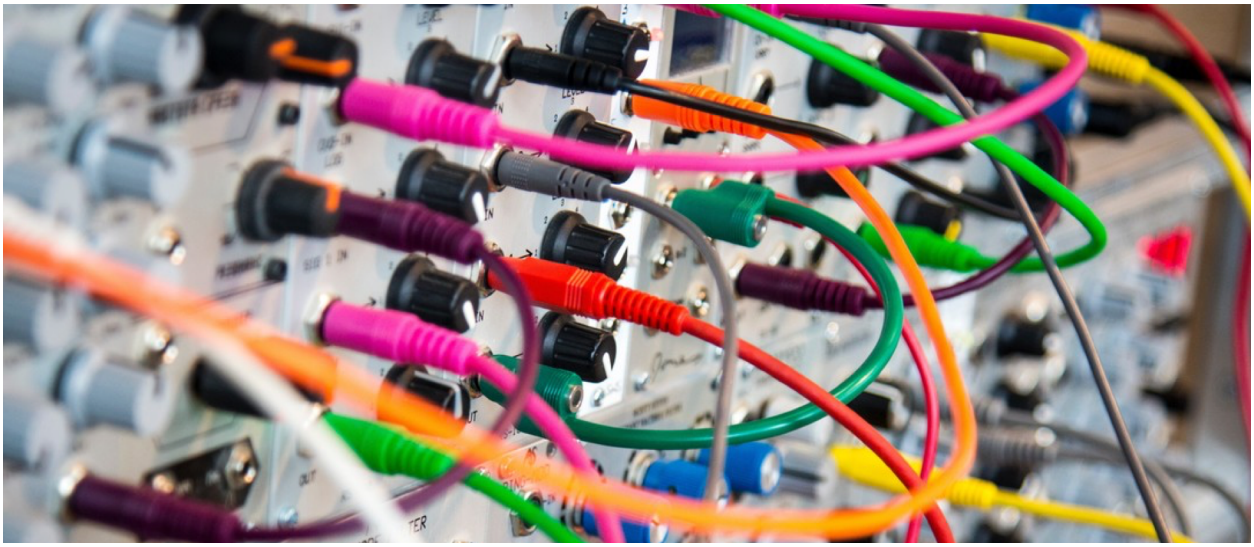
Conclusion: Avoid “Pull” Payment Methods

You have everything going for you as you grow your company and the services you offer, and as you build the financial infrastructure that will ultimately benefit everyone in your country.

Do not fall into the trap of adopting “Pull” payment systems!

Avoiding “Pull” payment methods does not mean there will be no fraud; however, it will be easier to protect your system against fraud and minimize any potential damage. In my fourth blog, I will start identifying where vulnerabilities exist, and what can be done to counteract them.

Part 4: The Weakest Link in the Transaction Chain



Sept 18, 2018: Nick Brown, International Payment System Expert & Founder of Clear Purchase

Every payment system is vulnerable to payment fraud.

In the previous blog in this series, I described why “Pull” payment systems are so vulnerable to fraud, despite all the preventative measures that can be added. However, even “Push” payment systems are vulnerable to fraud -- just to a lesser extent.

In this blog, I will show you the process I go through when I assess a payment system for vulnerabilities.

“You’re a Pessimist”

Years ago, when I was describing my work to a friend, she called me a pessimist, since I was always looking for any possible way things could go wrong. That set me back a bit, as I loved the challenge of doing something very difficult, and doing it well.

A payment system is easy to build and run, if you only consider when everything works. The real job involves minimizing the likelihood of failure, whether accidental or intentional, and minimizing the impact when it does fail.

I look for that “one in a million!” possibility. This might sound excessive, until you consider the sizes of the systems I have worked on, where 1 million transactions per day would be considered small – so, as you see, that “one in a million” possibility happens every day.

If being this focused on protecting systems from failures and fraud is considered being a pessimist, then I take that as a compliment!

Interoperability Changes the Game

I will assume you represent a company in a developing country that offers financial services to your customers, and that you are considering connecting your system to other systems in order to facilitate transactions between the two. This is often referred to as Interoperability, and would benefit your company and your customers.

So long as you have a closed system, it is fairly easy to protect it from fraud. Any fraud that does happen would likely be fairly easy to identify and reverse because the entire transaction chain remains within a single system. Everything changes when you connect your system to others, as I described in the first blog in this series.

Your job is to understand the potential for fraud, and protect your customers, as well as your company, from the devastating consequences of a major attack.

Where to Start?

Here are some of the questions you have to answer:

- What types of fraud are there?
- How much fraud can happen of each type?
- What effect will the fraud have on my customers?
- What will my company have to do to manage the fraud?
- What can we do to prevent the fraud from happening in the first place?
- What will other companies do to prevent the fraud?
- Who will take responsibility for the fraud?

And the list goes on.

This sounds daunting, so where to start?

The Weakest Link in the Transaction Chain

Because your system and your customers are vulnerable to a fraud attack that could happen anywhere in the payment system, it is important that you have a full understanding of the entire network. Remember, the criminal players will be looking at the whole network, and will attack what they decide is the weakest point.

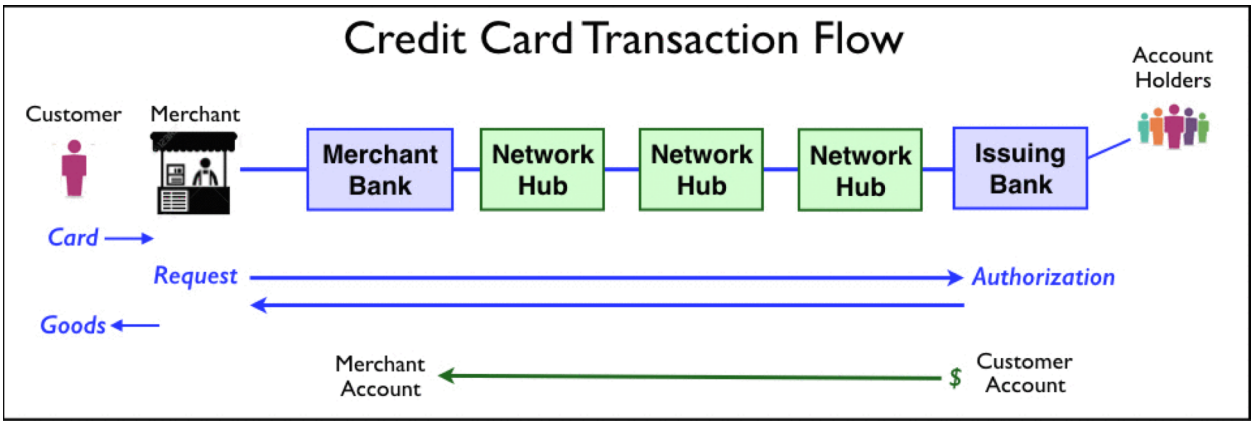
With 30 years in the industry, I am highly trained in identifying the vulnerabilities of any payment system. I also know that technology will continue to advance and that additional vulnerabilities will emerge and be exploited; so, this is a never-ending challenge.

I always ask the question: ***"If I wanted to break this system, how would I do it?"***

Below is a summary of some steps I generally go through when assessing a payment system. Once I find something of concern, I go into much greater detail to determine the true risks involved, and the actions that have been taken, or could be taken, to minimize the impact. In these steps, I will use a simple credit card transaction as an example.

Step 1: *Look at the flow of a typical transaction from end to end.*

A simple credit card transaction might look like this:



A customer inserts his card into a POS device at a merchant. A request is sent from the merchant through the card infrastructure to the customer's issuing bank, which authorizes the transaction and sends a response back to the merchant. At a later time, funds follow the transaction trail, from the customer's account to the merchant's account.

Step 2: *Ask: How easy is it to impersonate a customer?*

In a physical store, the impersonator would have to physically show up and present a valid-looking card, which, when run through the system, gets approved. This means either that the actual card was stolen from an account holder, or that a copy was made. The volume of this type of fraud is low, as an individual has to physically go to a store, and the imitator is often identified later and caught.

The bulk of card fraud happens online, where card information is entered onto a website and the transaction is processed and authorized. The impersonator does not need a physical card, just the card number and some additional information contained on the card. The impersonator can enter the information onto the website from anywhere in the world. This process can be fully automated, so millions of transactions can be submitted in a very short time. It doesn't take many successful transactions for this activity to be extremely profitable.

For "Push" payment systems, this is much more difficult, as the "Push" happens directly with the manager of the customer's account, which already identifies and authenticates the customer.

Step 3: *Ask: How easy is it to break into each system in the network?*

No system is impenetrable. The level of difficulty depends on the commitment of the system owner to data security. The banks and network hubs are in the business of data security, spending considerable amounts protecting their systems, so they are seldom broken into. However, merchants are in the business of selling goods/services, so they generally do only the bare minimum required when it comes to data security.

Actual systems are not the only vulnerable points on the network – the communication between systems could also be monitored, resulting in stolen transaction information. It might even be

possible to modify transactions as they flow between systems. Man-in-the-middle attacks would fall into this category.

Step 4: *Ask: What sensitive information does each system have about the customer?*

Once a system has been broken into, the easiest thing to do is copy data. The question is, what can be done with the available information?

For a credit card transaction, every system in the transaction trail has sensitive information about the customer - everything necessary to create fake transactions impersonating the customer.

If a system has sensitive customer information and is not well-protected, then there will be trouble. This is why merchants' systems are the primary target for credit card fraud, with high-profile instances like Target in 2013, when information from 40 million cards was stolen.

Something else to remember – it is entirely possible that the managers of a system might not even know their system has been broken into, if the fraud is only information theft.

Step 5: *Ask: What other damage can be done to each system?*

Once a system has been broken into, other criminal activities can occur, though those listed here are much more challenging to accomplish than simply stealing transaction information.

- Other sensitive information can be stolen, for example, routing information, passwords, and encryption codes – perhaps even the code itself.
- The system could be overloaded, causing it to grind to a halt.
- The data or code could be modified so that it processes transactions differently; for example, routing transactions in a different way, or changing fields, such as the amount field, within a transaction.
- Completed transactions could either be modified or deleted, or, fake transactions could be added.

Other than simply stealing information, these activities are generally fairly easy to notice and correct.

Step 6: *Ask: How easy is it to imitate a system within the network?*

Another major risk is the imitation of an entire system. While this is generally incredibly difficult to accomplish, the consequences could be catastrophic.

Imagine that all funds in your system that should be received for the day are instead sent somewhere else, from where they cannot be retrieved. That would be devastating!

A more likely scenario is that a transaction request is sent into the network as if it is from your system. This should be noticed fairly quickly, though maybe not until end-of-day settlement; however, a lot of fake transactions could be submitted before that happens.

What about a completely fake account issuer? Imagine a merchant you support accepting a transaction from a fake customer at this fake account issuer, who then authorizes the transaction. From your perspective, this would be a valid transaction, though no funds will be forthcoming. Neither you nor the merchant has any control over this.

It is important to determine how much these actions would damage you or your customers.

It's all about Minimizing Risks

These questions are intended to identify vulnerabilities, and then find out how well they have been addressed.

The goal is to minimize the likelihood of a failure, quickly identify when one happens, and then minimize the consequences. We are talking about a network, so there must be a clear declaration of responsibilities for each company in the network: what they must do, the options available to them, and procedures to follow in the event of a failure, as well as their clearly defined financial liability in that instance.

Fortunately, the majority of the above vulnerabilities can be fairly easily addressed, so that an attack is extremely difficult and would be noticed immediately. Fraudulent transactions would then be stopped as they happen. For those fraudulent transactions that slip through, find out how quickly they might be identified, and what countermeasures would be taken to shut down the breach and then reverse the transactions.

Unfortunately, all it takes is a single vulnerability and one major fraud attack for the whole network to come crashing down.

An example: Consider the possibility of a systems imitating a bank in a network that sends fake messages to a payment hub; the messages appear to be from a real bank that is already part of the network. It is the responsibility of the payment hub to ensure the authenticity of the source of every message they receive, through, for example, source identifying, encryption, message sequencing, or echo testing. Next, what if the payment hub doesn't do a good enough job of monitoring sources of messages, and fake transactions start being accepted? What backup processes are there to identify a breach as soon as possible? Finally, who takes on the financial liability of fake transactions? Because you have no control over whether any of these measures are actually taking place, the last question about financial liability is the most important.

The right questions to ask

It all comes down to knowing the right questions to ask, in order to find out what is being done to address potential vulnerabilities.

It's the job of the ***payment hub company*** to answer these questions. ***They*** need to convince ***you*** that it is safe to connect to their system. Do they have professionals with deep understanding of this industry working for them? Having quality people from other industries working for them is not sufficient, as the consequences of a single mistake are too high.

YOUR job is to identify the quality payment hub companies, and avoid the dangerous ones.

Start asking these questions now. The more questions you ask, the more your understanding of this industry will grow, the easier it will be to recognize quality payment hub companies, and the more confidence you will have when you finally connect to one.

Summary: Proceed with Confidence

Now that you know some of the right questions to ask, you will become better and better at recognizing the safer payment systems, and avoiding those that are a danger to your customers and your company.

Only connect to payment hubs that can show a deep understanding of this industry. They must clearly identify the vulnerabilities across the entire transaction chain, show how they have minimized the potential for failure, and minimize the impact if a failure were to happen.

When you fully understand all the risks, you are then able to move forward with confidence.

The benefits of interoperability are staggering for you, your company, your customers, and everyone else in the network. Your entire country will benefit. So ***Proceed with Confidence!***