We’re currently in the midst of the Digital Transformation, a roughly fifty-year length of time in which organizations and individuals will witness a dramatic growth in their reliance on digital technologies. The Digital Transformation is altering our lives in many positive ways.

For example, we can now have relationships and maintain constant communication with anyone anywhere in the world. Also, we can now order essentially anything from the comfort of our homes.

Businesses have more ability to grow their companies quickly. They can have stronger, more intimate relationships with customers - all while selling their goods to a much larger base of people.

With the good, always comes the bad. The Digital Transformation has increased risk to businesses because of things like identity fraud, social engineering, and data theft. In certain regards, the Digital Transformation is benefiting the bad guys as much as it’s benefiting the good guys. In some ways, more so.
FRAUD REALITIES

Online fraud has serious consequences for businesses. It increases business risk, eats into sales revenue, and is a noticeable day-to-day distraction to already busy businesses / business owners. It takes time and effort away from what’s most important: generating sales growth, shipping goods, and satisfying customers.

Because of online fraud, businesses are forced to invest in costly and time-consuming manual reviews. They also face the constant threat of chargebacks, stolen merchandise, unnecessary shipping expenses, and lost sales. All of these are no different than stealing cash directly out of the hands of hard-working merchants. It’s extremely frustrating, but it’s also today’s reality. This is why constantly studying how to minimize online fraud is a prerequisite for today’s ecommerce veterans.

TYPES OF FRAUD

While fraud comes in many different forms, there are common variations being used daily. Being able to quickly identify the first four will help you understand what you’re up against. The last two types of fraud hurt legitimate businesses: they defraud consumers and make them leery of purchasing online at all.

Identity Theft – This involves stealing the personal information of a victim through many different schemes, then making purchases fraudulently.

Friendly Fraud – This is when a transaction is completed and the customer (criminal) denies the charge in some way.

Clean Fraud – This occurs when a customer (criminal) uses a stolen credit card or account and proactively circumnavigates fraud detection.

Affiliate Fraud – This comes in a few different forms, including signing up for a program and then manipulating traffic or sign ups in order to get benefits that are fraudulently earned. This can be done with an online robot, code, or real people.

Merchant Fraud - This is simply providing a fake storefront to harvest credit card data from unsuspecting consumers. Often, low prices are offered in order to entice a person to use a site they have never heard of before.

Triangulation Fraud – This is a hybrid example of Merchant Fraud, the fake storefront lures customers with low prices to harvest their data, and they actually deliver the sale items through a real ecommerce site. At the same time, the fraudsters will use the card data to defraud the customer.
WHO ARE THE CRIMINALS?

Cybercrime is a burgeoning field, because it’s lucrative and, honestly, it’s difficult to prosecute perpetrators. In-store theft can be simpler to manage because you have a criminal physically on the premises. Not so much with cyber fraud. Cybercriminals can more effectively stay in the shadows, and they can easily band together, across the world, to commit crime. The basic inventory of digital criminals includes:

**The Experimenter** – This newbie criminal is dipping their toe into the waters of fraud. They may be doing it for a thrill or just to see if they can get away with it. If they’re successful the first time, they will do it again.

**The Low Ethic Individual** – These criminals have no concern about the merchant, or anyone else in their path. Their profile does not include high end technology crime, they are more likely to just order and try not to pay.

**The Repeat Abuser** – The repeat abuser is the experimenter who is developing a taste for the work. Maybe they commit fraud for supplemental cash or to score merchandise they otherwise could not afford. They often learn how to purchase or steal identities so they can be more proficient.

**The Individual Professional** – They’re generating serious profit from cybercrime, and it’s becoming less of a hobby and more of an occupation. This is when the criminals start to be very dangerous to businesses because from this point on they use advanced techniques.

**Semi-Organized Teams** – The next step for an individual professional is to band together with a few other online criminals. There are a number of reasons including greater opportunities, better use of tools or shared resources. Teams like this often strike at a greater number of businesses and more lucrative targets.

**Organized Crime (Mafia 2.0)** – This isn’t your godfather’s mafia! Mafia 2.0 specifically commits cybercrime because it is possible to commit the crimes anywhere in the world and the odds of being apprehended are so low. Like the mafia of yore, individuals play specific roles that help funnel money into the organization. Occasionally, these “families” also have connections to nation-states. Current research shows that 80% of cyberattacks are now committed by cybercrime rings.(1)

---

THE FUTURE OF DIGITAL CRIME

Digital crime is not going away anytime soon. As our reliance on technology increases, so too does our vulnerability. Cybercrime is currently one of the most profitable industries in the world. There are no signs of that changing anytime soon.

So, what does the future hold? Well, for one, we'll see an increase in social-engineering attacks, both physically and virtually. Bad actors will use their growing cache of personal information about us to defraud people with seemingly legitimate requests. Cybercriminals will become increasingly organized and their attacks will become more sophisticated and targeted.

Let's be clear, these things will happen, but it's not all doom and gloom. We'll invent new ways to authenticate transactions, so we can at least slow down some forms of fraud. We'll create more robust laws that police cyberspace and punish cybercriminals, and make a stronger effort to protect our digital assets, ourselves, our customers, and our organizations.

Businesses have to focus on today, however, tomorrow will come soon enough. In the final section, we'll examine how you can build a strong fraud strategy and create partnerships that will keep you and your organization secure in cyberspace.
DEVISE A WINNING STRATEGY

The past ten years have taught us many lessons about managing online fraud. There's no way to stop criminals from trying to target you, so the best strategy is to proactively and diligently use the tools at your disposal. You can't just pick one or two from this list; you must use all of these to minimize negative impacts.

Team training on fraud attack methods: Education is the first line of defense for any business. The more your employees know about how online fraud happens, and who the criminals are, the more easily they will spot issues before they become a real problem. Before an order leaves your warehouse or office, there must be at least one person who looks it over for the final time before shipping. Education is inexpensive and effective, but only if the curriculum is complete and carefully delivered.

**Action Item – Build or upgrade your existing training program. Make sure that any employee involved in taking, approving, or shipping orders attends the complete training session.**

Fraud software: There are a handful of good fraud-detection software applications. These tools do a great job of automating some of the testing that you would otherwise have to do by hand. Some platforms also keep a black list of contact data, so it's easy to spot known stolen identities or false addresses. These platforms continue to get stronger, so look for one that will be around for the next ten years.

**Action Item – Implement or upgrade to some type of fraud-filtering platform. In many cases, they pay for themselves over the course of a few months.**

Choose the right transaction partner: All transaction partners are not equal. Look for a partner who has a free program that help protect you against the common types of fraud if you follow their stated parameters. You want someone who is on your side and cares that you're risking losses every day.

**Action Item – Make sure you're taking advantage of all the programs and services partners are offering you. Once you're comfortable that a partner will work with you and is on your side, stick with them. Programs are improving all the time so stay up to date on the current benefits offered.**
Build a sophisticated fraud financial model: For many businesses, the reality is they will not be able to be fraud free without also throwing out good orders with the bad. The goal of never getting hit with a fraudulent order might drive you to cancel many legitimate orders that might trigger your alerts. Based on your profit margin and the average transaction amount, and a few other variables, you might shift your risk model up and down at different times of the day, week, or year. There's a perfect point between the risk of accepting all orders, including the fraudulent ones, and turning down everything that has the smallest inconsistency. You must be a master at flowing your risk levels actively based on factors you learn about along the way.

**Action Item –** Use your fraud platform, or a model you build yourself, to understand the risk/reward model for order acceptance. Teach you team members about the risk model and how to adjust it based on the factors that change your risk levels. Make conscious decisions on the kinds of orders you are willing to accept, and the ones that go nowhere.

Build a clear understanding of the fraud demographics you face: There's a science to understanding when fraud is most likely to happen, what products might be targeted, and where the shipping addresses might be from. Each of these factors (and a few others) will change the likelihood of fraud. Once you understand them, you can adjust your willingness to accept orders that have one of the danger factors you’ve learned. This is a perfect area to add to your training. Once the team understands these fraud demographics, you’re one step closer to building a model for when you might accept orders that have a red flag or two, and when you would absolutely turn them down.

**Action Item –** Attempted and successful fraudulent orders need to be tracked so the data can be analyzed over time. If you cannot answer the following questions at this point, put a plan in place to gather the data you need in order to answer questions like these:

- What time of day is fraud most likely to happen? Least likely?
- What parts of the country do most fraudulent orders ship to?
- What kinds of products that you sell are most ordered with fraudulent credential, or denied later?
- What dollar size of orders is most likely to be fraudulent?
- What day of the week is most likely to have fraudulent orders placed?

We’re Here to Help!

You don’t need to do this alone. You shouldn’t do this alone. PayPal has technologies and strategies that can help you mitigate fraud. We’re here to partner with businesses to combat the increasing risks of fraud. Give us a call and let us know how we can help you.

888.366.6386