Sometimes events in the payments world are seismic ones. A rumbling, a shakeup that puts everyone off balance and then the regrouping. The aftershocks are what need watching.

So it is with Equifax. No need to go over the numbers tied to the seismic breach here because they keep changing — and may be changing even as you read this eBook. When the impact stretches across oceans, nations and demographics, and those affected number in the hundreds of millions, a sea change is a-swelling.

Equifax brings a few key questions to mind. First: The proverbial (data) cat is out of the proverbial (ostensibly safe data warehouse) bag. That cat’s never coming back. Beyond the metaphor, the sheer “hugeness” of the data breach means that more information — and it needs to be stated that this is sensitive and valuable information ranging from Social Security numbers to birth dates to home addresses — is available to hackers than ever before.

If the rule of thumb for individuals is to assume that their data has been stolen, what are the new rules of thumb for companies transacting with those individuals? How should they adjust to a new reality where the data they are presented looks legitimate but may be stolen? How do they make decisions about retail transactions, lending activities or money transfers in milliseconds?

PYMNTS asked nine executives from a cross-section of the payments industry for their thoughts on how Equifax changes everything … and how it doesn’t. After all, companies must still look at what data is flowing into and out of their firms. They must still endeavor to keep consumer and cardholder data (and their own corporate data!) safe. They must also, in looking at transactions and customer interactions, try to foster a seamless experience. How to do that in an environment when just about everyone can agree the security status quo is no longer appropriate?

The executives we surveyed offered a range of ideas on how businesses should move away from what may have been a “one-size-fits-all” approach. Currencycloud CTO Ed Addario argued that regulation may in the offing, but emphasized that firms must also strive for speed and transparency in dealing with breaches. ICBA Bancard President and CEO Tina Giorgio offered some insight into what firms did after news of the Equifax breach hit. In almost all cases, the need for eternal vigilance was stressed.

Yes, October may be National Cybersecurity Awareness month, and headlines may flare about what to do and what not to do, but when it comes to protecting data, all too often we forget until we are reminded. And when it comes to protecting sensitive data, all stakeholders — from consumers to corporate back offices — must be conscious not to be unconscious.

Read on….
Due to the size and seriousness of the Equifax breach, it certainly causes one to consider the implications and learn (or be reminded of) some valuable lessons. For myself, three thoughts immediately came to mind.

First, as someone who’s lived in the payments ecosystem for years, the breach only underscores the importance of security. Personally identifiable information (PII) is the same as payment card holder info and anything else we need to protect, in that, when we’re storing it, we need to take every precaution we can.

That said, my second thought is that this breach highlights that it doesn’t matter if you’re big or small — we can assume that a company the size of Equifax has a significant security budget — you’re still vulnerable to the same attacks as everyone else. The breach reinforces the need for good digital security hygiene that includes a perpetual attention to things like patches, access control evaluation and vulnerability testing. Big or small, companies have no excuse to ignore security or not take it seriously.

However, I do have sympathy. I recently attended the Black Hat USA 2017 conference in Las Vegas. This show brings out the most passionate and skilled people in the security industry. What they can do is both amazing and frightening.

“Security is constantly evolving — and faster than ever.”
Now consider how these people don’t have the resources of the highly motivated countries or criminal organizations behind today’s biggest attacks. The primary threat is no longer kids running scripts and hacks they downloaded. Governments and organized criminals have bleeding-edge technologies at their fingertips that the mainstream hasn’t seen. How can we hope to defend against such enemies? This brings me to my final thought on the matter.

Security is constantly evolving — and faster than ever. A security stance today might change tomorrow or an hour from now, since new issues and exploits pop up all the time. Vulnerability exploits have been weaponized, and the tools evolve daily. There’s a shadow network of people across the world with massive amounts of money at stake.

With all this in mind, today’s security teams face stiff challenges and can’t rest for a second. Our security teams must be actively engaged and working against criminals 24/7/365. If financial or personal information is at stake, we must be ever vigilant and constantly evolving to match the evolution taking place by our criminal counterparts. Anything less will result in additional breaches and PII loss.
With approximately 150 million individuals’ personal information in the hands of criminals, as well as over 200,000 credit card numbers stolen, Equifax’s data breach will go down as the largest in U.S. history — at least for now.

Details on how this massive data heist was performed are still scarce and sketchy, and we may never know exactly how so much data went undetected for nearly three months from one of largest credit scoring companies in the world. However, one thing is certain: Equifax’s security policies and cyber defenses proved to be woefully inadequate, and that is a sobering thought for anyone, not only in the financial services industry but anywhere where personal information is stored electronically. That is, everywhere!

While I can sympathize with Equifax, I think it is inexcusable that they delayed disclosing the breach for so long. The now-former CEO’s explanation of not wanting to attract further attacks strikes of an incredibly naive, or profoundly misguided, sense of care.

“Openness and transparency will go a long way in mitigating the effects.”
In my view, regulation is seldom the answer to corporate failings, but in this case, the data breach provisions included in the General Data Protection Regulation (GDPR) — the enhanced directive intended to strengthen and unify data protection for all individuals within the European Union — feel timely and necessary. While the regulation, which goes into effect in April 2018, will impact U.S. companies that offer goods and services to EU citizens, the standards it sets for reducing risk exposure should be on the agenda of all American institutions.

In the next few months, we will see congressional hearings, TV talking heads interviewing security experts and an endless stream of articles on what went wrong and how to avoid [the next breach]. No doubt good insights will come out of it, but I cannot help but feel that in the end it will boil down to the basics: data at rest encryption, proper access control, all IT infrastructure updated with the latest security patches, segregation of roles and responsibilities and common sense. The most important lesson to be learned, however, is: Do not delay informing those affected. Openness and transparency will go a long way in mitigating the effects.
Anytime there is news of a data breach, it creates uneasiness among consumers and any company that handles sensitive data. Breaches like the Equifax breach serve as critical reminders to us all on how important data security is and cause CIOs like myself to continually re-verify our systems are as secure as possible.

The approach we have to data security doesn’t change at a high level due to the breaches we hear and learn about. Of course, we monitor these events and learn any valuable security insight we can from what is happening in the market and in our industry. We enhance our programs based on this key learning. However, these events only reinforce our commitment, with resources and technology, to ensure that our environment has all of the necessary safety protocols in place.

As I’ve talked with other CIOs and around our industry, a common discussion is on the suite of tools used for keeping data secure. Our approach regarding data security at First American is not a one-shot approach. Our team uses multiple tools and programs that together provide a meshed environment. This ecosystem employs a defense in depth strategy in which there are multiple layers of security that all work together to form a very strong barrier around sensitive payment data. If one layer shows weakness, it’s quickly balanced by the other layers we have in place.

“ The most important thing any business can do is to deploy a set of tools and programs in a meshed environment in order to protect the data collected and stored.”
As a part of this defense in depth strategy, it’s critical to also monitor outbound traffic and data with data loss prevention tools, in addition to monitoring the inbound traffic. Our security tools monitor both directions of data traffic to ensure it’s secure and keeps cardholder and other sensitive data safe. By looking at both inbound and outbound traffic and ensuring our meshed environment covers both, we feel confident that our data is secure.

As you can see, we believe that no one tool or defense will protect sensitive data. The most important thing any business can do is to deploy a set of tools and programs in a meshed environment in order to protect the data collected and stored. Without these tools in place and working together, companies open themselves up to data vulnerabilities, as we have seen in the marketplace.
"The Equifax breach is yet another reminder that a data compromise can always be around the corner."
By asking questions — such as, “At what branch did you open this account?” or “What was the date and amount of your last deposit or loan payment?” — we can dramatically reduce the likelihood of a bad actor compromising a customer’s account and identity. This is paramount for community banks, whose reputations and relationships with customers are built on trust.

Multi-factor authentication is presently our strongest defense against these vicious attacks, because it confirms a user's identity by combining several variables that typically fall into one or more of the following categories: knowledge (something I know); possession (something I have) and inherence (something I am).

Security protocols that comprise multiple layers of protection tend to be more effective at combating fraud. As technology becomes more sophisticated and consumer demand spurs innovation, authentication measures that include possession and inherence (in practical application, think tokenization and biometrics) will make up more of the factors in multi-factor authentication.

The Equifax breach underscores the fact that no organization that is responsible for safeguarding consumer information can ever be too prepared when it comes to security.

Community banks will remain vigilant in today's cyber landscape. The Equifax breach is yet another reminder that a data compromise can always be around the corner. However, community banks will continue to protect their customers to the best of their ability and communicate important and timely information to them as soon as possible.

By partnering with their customers during times of uncertainty, community banks will continue to take an active role in helping to mitigate fallout for their customers from these vicious cyberattacks.
"Consumers need to take charge of their world, before someone else does."

The Equifax situation should put all consumers on heightened awareness, and identity and credit protection should be everyone’s top priority, regardless if their information was involved in this breach or not.

Too much personally identifiable information (PII) is readily available, whether it’s on Facebook or the dark web. There is nothing positive about the Equifax breach, but it has reinforced that data security and consumer protection need to be a continued and targeted topic of conversation to drive change in security practices. There is no easy fix, but consumers and businesses can take steps to mitigate the risk.

Consumer awareness is the first step. Consumers need to take a proactive approach to monitoring their sensitive information. Locking down Social Security numbers with all credit bureaus is a simple and easy step that helps protect ones’ identity. Consumers can also take advantage of free credit reports to watch for fraudulent account creation. Continuous surveillance of online accounts should be part of a recurring routine so that any account takeovers can be caught early.
In the typical call center environment, the natural desire for the representative is to take care of the customer — not to be a fraud analyst — and this can lead to inadvertent skips in business processes. Agent security education should be a recurring and integral part of the climate and culture of the call center. Call center IT personnel should continually explore the most up-to-date technology to limit internal and external exposure to PII.

There are different technologies that exist to secure data, and traditional multi-factor authentication (MFA) will remain an important part of security. MFA continues to improve with enhanced technologies, such as voice, fingerprint, retinal and facial recognition biometrics.

Additional security options for call centers are proactive threat detection with real-time call authentication, call origination forensics and customer-driven inputs in live environments. These are strong and viable options in the quest to protect consumers’ information.

With that being said, there are other concerns in a call center environment that warrant mention:

- Customers providing PII during open-air communications (bus, train, etc.)
- Decreased customer confidence when verbalizing PII
- Back-office access to quality monitoring recordings
- Rare, but still present, internal bad actors

There is no easy answer and no one-size-fits-all approach to identity and credit protection for either consumers or businesses. Both have a shared responsibility; however, the true change agent in protecting consumer identity is education of the consumers themselves. Consumers will ultimately demand that industries involved in handling PII engage in more stringent protection and handling, and businesses need to be ready to accommodate these demands. Consumers need to take charge of their world, before someone else does.
How Do You Share a Secret?
You have a secret that only you know. If you keep that secret to yourself and tell no one, then there’s no problem — no one else in the world knows what you know. But what if you have to share this secret? Who do you choose to tell? You may find someone who you trust with this secret. But how do you exchange that information? Do you tell them in person, face-to-face? Do you whisper it to them over the phone? Do you write it on a piece of paper? Do you text it? Do you email it? What is the most secure way to share the secret without anyone else listening in or reading over your shoulder?

The reality is that as soon as you share a secret with someone else, it is no longer really a secret. It’s not as secure or as safe as when you kept it to yourself. The problem with keeping secrets is that needing to share them makes us vulnerable. The most recent example of this is the unfortunate breach at Equifax, which occurred because the company is in the business of exchanging sensitive data, and, by definition, is sharing secrets that are potentially exposed in transit.

With Great Power Comes Great Responsibility
Data is power; by adding context you can create information, and information, in turn, can help one make better decisions. But with great power comes great responsibility. Almost all companies are responsible for exchanging, managing and securing some data in their custody. When handling and sharing their data, sometimes they overvalue it, sometimes they undervalue it, sometimes they hoard it and (unfortunately) sometimes they squander it.
And as with Equifax, some of these companies aren’t able to keep their data safe and protected from those wishing to misuse it. In this way, being responsible for data is also a double-edged sword. When faced with the downsides of that double-edge, many companies retreat and look for ways to stop exchanging data.

That is too bad, because, for the most part, sharing data makes the world a better place for everyone. For instance, knowing more about customers (via data sharing from different pools of data) actually enables better protection of that very data, because when the data is misused, it is more readily identifiable. In payments, data is different from most other kinds of data, and its value comes from efficient (and secure) exchange of data.

Payment event data (the data related to the actions to prepare, execute and warehouse the data) is unique as it has special requirements for security. It’s used within financial systems as the basis for accounting. It describes the state of the relationship of the sender and receiver. It is embedded within the most important processes of every business. And, truly unique, it’s never owned just by a single party and so must be shared! Therefore, when data breaches cause companies to retreat from exchanging data, payments events don’t work as well as they could, should or need to [in order to] create the seamless experiences that customers want.

**Next Steps to Security**

So what is a potential way forward? It all comes down to the way that we have approached “the right” to use a specific customer’s data. Most companies today ask their customers to agree to provide them rights to the data (that customers actions produce with that company) in a “block grant” all-or-nothing approach. This approach is made worse by the open-ended and vague “potential” uses of the data that the legal agreements stipulate.

There is a better way to do this. Customers should not have to hand companies “carte-blanche” rights and should be asked for permission to use specific data for a specific purpose on a case-by-case basis. This is 100% technically feasible. Today’s always connected, smartphone enabled, real-time feedback culture is also ready. Of course this case-by-case request for permissions puts the burden on companies to succinctly explain the value proposition that they want the customer to accept. As a block, it is practically impossible to make consistent rational decisions about data. On a case-by-case basis, the right answer can almost always be quickly determined by the customer. Companies might be surprised just how often people will say yes. When customers understand the value of individual exchanges of data they will be better participants in the data sharing ecosystem. They will keep companies focused on the value of the exchange to their customers as opposed to the company (only). This process can also help companies understand more about what their customers value and then relate with them better in the future. Over time this will increase the confidence that the customer has in the company and very well may result in larger “bulk” agreements to data sharing. More data will be shared more intelligently and will help us all work better together. Especially in payments and the events they represent!
The Equifax data breach sent shock waves through the cybersecurity community. But despite its scale and the subsequent breaches at the SEC, Deloitte, Sonic and others, most companies will likely do little more than marginally increase their 2018 cybersecurity budgets. Which leaves consumers right where they were before, with their data just waiting to be stolen.

**New Account Approvals**
The biggest implication from a breach of personal data for 143 million Americans is for companies who approve credit based on that data. This includes issuers and payment processors who offer “instant” credit to consumers, as well as all retailers who offer “instant” credit as part of their checkout process.

Until it’s clear what happened to the Equifax data, it would be wise for eCommerce merchants to strictly monitor and curtail the approval limits on “instant” credit offerings. On a broader scale, the same is true for all new accounts and even guest accounts where new credit card details are being added.

**The “Lone Wolf” Cybersecurity Strategy**
One thing online retailers, regardless of size, must not do right now is try to face this threat alone. Merchants need to work with their fraud
protection platform providers and leverage all possible assistance available from the cybersecurity ecosystem. There is no “lone wolf” strategy for cybersecurity. Fraudsters prey on eCommerce sites operating with limited data and manual order reviews. Going it alone simply leaves your customer data vulnerable to threats — threats your platform provider may already be aware of.

As an example, Signifyd’s global network of 5,000 merchants and our partnerships with the world’s leading third-party data sources provide a 60 percent chance that Signifyd has seen a consumer before they place their first order with one of our merchants. Thus, now, more than ever, merchants should partner with their platform providers to leverage real-time knowledge of which consumer accounts are being operated by fraudsters and which are perfectly legitimate, despite what may appear to be “unusual” activity.

**eCommerce Fraud**

Given the magnitude of the data breach, some risk experts may expect a spike in stolen financial fraud or account takeover fraud. But neither has spiked immediately following the breach. What may be even more surprising is that account takeover fraud was already rising rapidly in certain eCommerce verticals before the Equifax data breach.

In early July, analysis of account takeover fraud losses for Q2 2017, compared to a year earlier, revealed an alarming trend: 55 percent increase in apparel, 87 percent increase in consumer electronics and a staggering 138 percent increase in cosmetics. While the addition of over 200,000 stolen credit cards doesn’t help matters, it also doesn’t change that much in the already-thriving black market for stolen financials. Thus, merchants need to stay focused on growing fraud threats that were already emerging and are now exacerbated by the Equifax data breach.

Some financial institutions and online retailers will act now and have likely already taken steps to strengthen their authentication and verification methodologies. These are the early adopters of cybersecurity best practices, and the Equifax data breach will deepen the divide between those who are secure and those who aren’t. Those with more to lose (larger merchants, better-known brands) are more likely to strengthen their security quickly, as they wish to demonstrate a safer, more secure online shopping experience for their customers and to ensure they are not the next breach to make headline news.

In this regard, the recent string of breaches has created a unique opportunity for savvy online retailers to set their brands apart by strengthening their security protocols.
This is an interesting question, as the Equifax data breach is going to hugely affect a significant majority of U.S. citizens; however, I expect only a small amount of the population will have taken notice of what has happened and have correctly interpreted what this means for us personally.

I don’t want to generalize too much, but a large number of millennials are blissfully unaware of the dangers of data breaches, having never felt the impact of one before. Without realizing it, they have a higher risk tolerance than those who are switched onto this kind of criminal activity or have experienced first-hand the implications of some of the newsworthy breaches, such as Target or Home Depot. The Chipotle data breach earlier this year did not dissuade many from satisfying their craving for guacamole.

The Equifax breach has sent a shiver down my spine, as both a consumer and a security professional. When sensitive financial data, such as credit card information, falls into the wrong hands, we can limit the impact by canceling the card and requesting a new one.

In this case, it’s our personally identifiable information (PII), such as Social Security numbers, which cannot be changed; so, the effects of this breach will be felt now but also over the long term, as criminals repeatedly dip into this data. According to the Federal Trade Commission, they estimate it takes an average of six months and 200 hours of work to recover from identity theft. I am pretty sure that no one wants to give up that amount of time.

“The Equifax breach is a worst-case scenario, and it effectively demonstrates the direction criminals are going in.”
Vigilance is going to be the keyword going forward. I do not trust anyone with my PII at this point. I no longer allow eCommerce websites to hold my credit card information on file for future purposes. I have changed from allowing them to be the custodian of my data to now taking precautions and monitoring who has what.

I recommend setting up text alerts with your banks and that you check your accounts weekly to ensure that all transactions showing are correct. I would also put credit freezes in place and unfreeze them only when necessary, which will hopefully reduce your vulnerability if your PII should be targeted. And finally, I recommend using two-factor authentication across your accounts to tighten security further.

The Equifax data breach highlights that security is not as strong as the will of the criminals. It has become a job for them and the source of their livelihood. They are subject matter experts and have time and resources to identify and exploit weaknesses in company defenses. They band together and share information on the dark web for the potential money-making opportunities associated with selling PII on the black market. Most companies struggle with security, so it is essential they understand what they can handle and what they need to offload to service providers trained to combat threats.

Service providers need to up their guard too, and this is where the payments industry can do a great service to others, as we have been on the front line for many years. The history of the payments industry, a key target for criminals, is littered with breaches, and with each new threat we have tightened our defenses.

PCI-DSS has been an effective way of ensuring a certain standard is met and strict controls are in place for the payments industry. Security enhancements, such as the introduction of the chip in EMV-compliant cards, have made it difficult for hackers to duplicate cards. With our diligence in the payments industry, the hackers are finding it hard to target payment card information, so they are now turning their attention to PII, which is non-cardholder data related.

PCI-DSS has requirements which are prescriptive. Do we have anything out there today that protects consumer PII within the commercial sector? The Equifax breach is a worst-case scenario, and it effectively demonstrates the direction criminals are going in. Find the weakness, and attack it.

Collectively, the payments industry should feel proud of the strides we have made in our security measures; however, the Equifax breach shows that criminals will continue to surprise us with their ingenuity, so we need to keep our eye on the ball, respond to new threats and set an example which other industries can follow.

As a U.S. citizen, I can only lament Equifax’s lack of security measures and hope that the far-reaching implications of this breach will be minimal for my friends, family and acquaintances; although, as a security professional, I know the chances of this are small, and I’m preparing for the worst.
As a global service provider within the identity landscape, the importance of protecting personally identifiable information (PII) is always front of mind. Any time a breach involving the misappropriation of sensitive data occurs, we are reminded of the importance of doing everything possible to defend against a similar potential breach.

The recent Equifax breach serves as a timely reminder that the maturity of an organization’s information security system often comes down to the most rudimentary policy and process. Breaches are as much a failure of protocols as they are of network security systems. So, it is becoming exceedingly important to ensure businesses and organizations are regularly revisiting fundamental questions, such as: Are our system update processes adequate? Is it clear who is responsible for the maintenance of each aspect within the Information Security Management System? Do we regularly train and educate our employees on various phishing attempts and acceptable use policies? Etc.

It’s also important to remember that the verification of identities can be done in many ways. Currently, Trulioo provides customers with an increasingly diverse toolset in regard to the data required to satisfy Know Your Customer (KYC) and anti-money laundering (AML) compliance requirements.

“The question that remains is whether or not it will also lead to a need for tougher regulations and, in turn, tougher penalties.”
In this digital age, identity is a combination of different attributes — both old and new — your name, date of birth, address, telephone number, email address, mobile and more. This consortium view of identity, that encompasses data from multiple traditional and alternative sources, highlights that any data breach is only as destructive as we allow it to be.

Looking toward the future, this breach will surely bring to the surface more security-related questions from the various regulators around the world and very likely [create] an intense ripple effect. This reaction is likely to be twofold: ensuring data protection standards are amplified and increasing the punishment for those who do not meet the necessary requirements and suffer breaches as a result. In Europe, regulators are already tightening their belts.

The General Data Protection Regulation (GDPR) is a series of laws created to strengthen and unify data protection for all European Union (EU) citizens. Various parties are required to develop and implement vastly refined data privacy handling procedures by May 25, 2018, or face penalties as high as 4 percent of global annual turnover. Last year, the three biggest credit bureaus grossed over $9 billion in revenue. If this breach were GDPR-related, a single breach could result in hundreds of millions of dollars in regulatory fines.

Now, the question is being posed as to whether similar laws and regulations will be implemented closer to home, and all signs point to yes.

Not only will the Equifax breach garner a reaction from regulators around the world, it may also see consumers demand greater control and transparency over how their personal information is handled. In the wake of the breach, Canadians were advised to be more vigilant about their personal data. There are many options that can be taken — for example, setting up fraud, credit and banking alerts that notify an account holder when there is irregular activity. And this is only the tip of the iceberg.

So, what can we learn from the recent breach? It’s obvious that better security leads to greater privacy protection, and a greater emphasis on the two leads to more efficient, secure and transparent protocols. The question that remains is whether or not it will also lead to a need for tougher regulations and, in turn, tougher penalties.
PYMNTS.com is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.