Equifax Data Breach

Implications for E-Commerce Merchants

November 2, 2017

Mitch Muroff
mitch@curaxian.com
+1 415 508 7094

Contents

Introduction

What E-Commerce Merchants Need to Know

Equifax has stated that "Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017."[1] Company sources added that "the information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[2] In addition, "Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents."[3] As for the magnitude of the breach, Equifax determined that a total of 145.5 million[4] accounts were affected.

Given the magnitude of this event, we believe it is important for e-commerce merchants to understand how criminals might use this information to develop new attack vectors and recommend that merchants should reassess their control environments for vulnerabilities to these new attack vectors. It is our view that failure to ensure adequate defenses against new forms of attack potentially enabled by this data could expose vulnerable merchants to unprecedented fraud losses and fraud-related costs.

The objective of this white paper is to describe how criminals might use the Equifax data to design new attack vectors, then discuss the types of compensating controls merchants can deploy to protect themselves so that merchants can develop a defense structure resilient enough to detect and resolve the types of attacks we expect to evolve as a result of this data breach.

The Breach

The objective of this section is to describe what happened and why it matters from a merchant perspective.

Data is the fuel that powers increasingly sophisticated attacks against merchants, costing them more than $60 billion per year in fraud-related costs.[5] This breach is not exceptional in terms of the number of records accessed or the number of individuals affected, however, the nature, quality, and value of the information that has been stolen is unprecedented. Criminals have long had access to stolen payment card numbers, but never before have they had access to so much high-quality identity data about so many consumers. What's more, this data has a long life. When a cardholder reports that their card has been compromised, the card can be cancelled by the issuer, rendering the number useless. The address of a consumer, by contrast, is valid for as long as the consumer lives in the same place. And, a consumer's Social Security number and date of birth remain the same for the life of the consumer. Furthermore, knowing a consumer's name, current or prior address, date of birth, and Social Security number could allow an attacker to obtain nearly any additional data about that consumer from other data sources, since those are the data elements typically used to authenticate and locate additional information about a person.

When a criminal obtains a stolen payment card number, they may or may not also get access to the name, address, and security code associated with that payment card. If the criminal has just one piece of information about the identity associated with a stolen payment card number, they can potentially join that data with the data stolen from Equifax to determine the complete and accurate identity of a given cardholder. For the 209,000 credit card numbers reportedly stolen from Equifax, criminals may not even need to make such an effort to get a complete identity for a payment card. If criminals can successfully purchase $5,000 on each of those cards, that data set could be worth as much as $1 billion to criminals, and might represent more than $1 billion in losses to merchants, who will pay for the goods that were sold plus fines, fees, and penalties assessed against the merchants by acquirers, payment processors, and card brands for accepting those transactions. And, as merchants tighten their controls to defend against these attacks, they will spend more money on fraud detection and manual review, and will be forced to reject more orders from legitimate customers due to the need for heightened acceptance criteria.

From a merchant perspective, then, there are two key facts that distinguish the impact of this attack from the payment card data breaches that preceded it. First, criminals now have an unprecedented opportunity to develop accurate and complete identities linked with the payment card numbers owned by those identities. Second, criminals have the potential opportunity to achieve this objective for as many as 145 million consumers, and the size of this data set may enable criminals to launch automated attacks of previously unimaginable scale.

Attack Vectors

The objective of this section is to describe how criminals might use the Equifax data to design new attack vectors.

We have identified three attack vectors that we believe are most likely to be facilitated by the Equifax data and refer to them as "High Scale Clean Purchases," "New Account Fraud," and "Address Changes."

High Scale Clean Purchases

It is easy for criminals to obtain large numbers of valid payment card numbers that can be used to execute fraud attacks against e-commerce merchants. In our experience, it has been comparatively rare to find fraudulent orders that also contain valid names and addresses.

Criminals have developed scalable attack technologies that allow them to evade many of the defenses merchants have historically relied upon to detect fraud. In recent years, we have served many high-profile merchants who found that existing fraud-scoring algorithms, velocity rules, geo-location rules, behavioral rules, and device-detection technologies are no longer able to effectively identify fraudulent orders.

In response to the fact that many standard technologies are not detecting fraudulent orders with contemporary attack vectors, we've seen an increase in the incremental adoption of technologies that validate identity data submitted with orders. In our experience, the introduction of data validation services into the merchant decision flow has been the most effective option for merchants to improve fraud detection. We have found these services to be highly effective in identifying fraudulent orders that otherwise would not have been discovered by detecting anomalies in the identity data provided with fraudulent orders.

If data validation is the last line of defense, then what happens when the data provided with fraudulent orders is also perfectly valid and passes these tests?

Criminals have already learned that they need to design orders with accurate names and addresses to pass identity validation tests adopted by merchants. The Equifax data provides them with perfect names and addresses for 145 million American consumers. This data will allow criminals to produce orders that pass identity checks at scale, and as such, will allow them to develop large-scale automated attacks that pass identity checks, which, to date, have been merchants' defense of last resort.

What's worse, we expect criminals to organize the available information into a structure that allows them to respond confidently when merchants contact them to verify orders deemed as suspicious and set for manual review.

New Account Fraud

New credit cards can often be opened online with nothing more than name, address, Social Security number, and date of birth as identifying elements. Issuers may verify that data against the very data sources that were breached. If an issuer verifies the data entered into an online application form against a database service provided by Equifax to determine whether the application is legitimate, it's likely the data provided by the criminal will match exactly.

Some issuers may require additional information before opening a new credit card account, but if a criminal already knows the correct name, address, Social Security number, and date of birth, it's likely they can use that data to obtain whatever additional information an issuer requests by cross-referencing the data they have with other data sources or using that data to authenticate and hack into other services provided by Equifax or Equifax competitors. Equifax has also stated driver's license numbers, which an issuer might use for additional authentication, were included in the breach "in some instances," thus reducing the efficacy of using a driver's license numbers for additional verification.

One might reasonably expect issuers to be aware of this heightened risk, and we hope issuers have developed effective control enhancements where necessary to protect against large-scale attacks of this type, but the if the criminals can succeed in opening only two cards (from different issuers) per stolen identity, that's 290 million new card numbers. If those cards have an average credit limit of $20,000, the total purchasing power of such an attack could be $5.8 trillion. With an opportunity of this size, even a miniscule success rate could be incredibly profitable to the attackers. There are many credit card issuers in the United States, and some of the smaller issuers may lack the resources to effectively manage a sophisticated campaign to open new accounts using the data stolen from Equifax, and if the larger issuers fail to stop even a small percentage of attempted attacks, the number of new cards, and the purchasing power of those cards, could be astronomical.

In turn, merchants may be subject to chargeback transactions and card brand chargeback monitoring programs if they accept orders from criminals who use account numbers using identity data stolen from Equifax. Even authentication methods provided by the card brands themselves are unlikely to protect merchants against these attack vectors, because the criminals will almost certainly be able to successfully complete any in-transaction authentication steps presented to them because they are the actual cardholders.

If the person whose identity was stolen contacts their issuer to state that the charges are fraudulent, then the issuer may charge the transaction back to the merchant, leaving the merchant with a loss, and exposing the merchant to fees and fines that may be imposed by their acquirer and by each card brand. If the merchant accepts too many of these transactions and exceeds card brand thresholds, they are subject to additional fines and penalties and could eventually be banned from processing card transactions completely.

We therefore expect an increase in fraud attacks on merchants using new cards fraudulently opened by criminals using the data stolen from Equifax. These attacks will be particularly challenging for merchants to detect because the criminal is the cardholder, so typical strategies used by merchants to determine cardholder authorization for the transaction are more likely to be passed by the attackers.

Address Changes

In an attack designed to illegally obtain physical goods for use or resale, getting access to the goods remains one of the biggest challenges to the criminals. Historically, criminals had to choose between placing an order with different billing and shipping addresses (a choice that exposes them to increased screening by the merchant) or shipping the goods to the cardholder's address, then trying to redirect the order after it's been shipped (a strategy that can be thwarted by merchants who direct their shipping partners to disallow redirection requests). Shipping the goods to the cardholder provides no value to the criminal unless the criminal is being rewarded for the transaction through an affiliate program.

If a card issuer allows a caller to change the address associated with a payment card after authenticating their current name, address, date of birth, and/or Social Security number, then it may become easy for criminals to use Equifax data to change the address associated with a payment card. Once this is done, the criminal can place an order with a name and address that matches that on file for the card, and ship the goods to the address associated with the card, thereby circumventing all merchant controls designed to look at orders where billing is different from shipping.

Since this process requires a lot of time and manual labor, it is not scalable, and is therefore not likely to be executed with considerable velocity. However, this attack vector may be economically viable for criminals seeking to design attacks with high expected value from relatively few transactions.

Controls & Defenses

The objective of this section is to describe the types of compensating controls merchants might deploy to protect against the new attack vectors described in the prior section, so merchants can develop a resilient defense to detect and resolve the types of attacks we expect to evolve as a result of this data breach.

Scrutinize High-Value Orders

Given the relative expense of opening new credit card accounts or changing addresses on file for existing accounts, it is our hypothesis that criminals will reserve these strategies for the highest value transactions.

When evaluating orders of exceptional value, consider the possibility that the card might have been opened by a criminal using stolen Equifax data or the card address might have been changed by a criminal using Equifax data to authenticate with the issuer.

One potential strategy to defend against this attack vector in the context of exceptionally valuable orders might include use of the "code 10" process to request assistance from the card issuer. A conversation with the fraud department of the card issuer might include asking for information about the account opening date for new accounts or address changes for established accounts. Consider new accounts or accounts with address changes to be higher risk. Consider asking the issuer to contact the cardholder to validate the transaction. Unfortunately, if the cardholder is the criminal, then this verification step may also fail to detect the fraud.

Another potential strategy is to pull credit history and look at the open date for the payment instrument being used in the transaction. The ability to deploy this strategy would be subject to appropriate regulatory constraints.

In the case of high value orders for physical goods, the criminals will still need a method to obtain the goods for resale or other method of monetization. If the criminal opened the account using the address of the person whose identity was stolen, then the criminal will have to choose between one of the following strategies to get the goods:

1. Change the address on file for the account so billing and shipping addresses remain the same and the order is not flagged for review on the basis of differing addresses, or

2. Ship to the address of the person whose identity was stolen but attempt to redirect the order after placing it so it is ultimately delivered to another location, or

3. Place an order where billing is not the same as shipping.

Changing the address on file increases the time and cost to the criminal, so this reduces but does not eliminate its viability. It will be very difficult for a merchant to protect against this method in the absence of assistance from the card issuer, and even then, the burden on the merchant to perform a code 10 with the issuer is not scalable. This

remains an attack vector that will be nearly impossible for a merchant to cost-effectively defend against and may turn out to be an area of considerable opportunity for criminals.

Criminals deploying an address change strategy may still be vulnerable to detection by merchants who use identity verification services because those services will not reflect recent address changes. Therefore, the new address will be flagged by identity checks as not matching the name in the time period between the address change and refresh of the data sources used by the identity verification service. Merchants will need an effective process to distinguish between the address change attack vector executed by a criminal and a valid address change from a legitimate customer.

Redirection can easily be stopped by the merchant. See "Prevent Redirection" below. This is an easy win.

It is already a best practice to scrutinize orders where billing is different from shipping. This attack vector will make those orders look cleaner and therefore underscore the need for merchants to be at the top of their game, but merchants who deploy best practices in evaluating orders where billing and shipping are different should be able to manage this risk.

Merchants offering digital goods or services are subject to considerably higher risk from attacks using accounts opened by criminals with stolen identities since there is no need for the criminal to establish a link with a specific physical address to receive goods. It is our belief, however, that few digital goods or services have sufficient value to be worth using an account created with a stolen identity. For merchants that don't ship physical goods, the greatest risk resides with those who provide services of exceptional value. Airlines, for example, may face intensifying attacks involving purchase of high-value tickets in premium cabins with short lead times to departure. Merchants in the digital or service space should therefore carefully evaluate existing controls to determine whether there are sufficient compensating controls in place to detect exceptionally clean orders with completely matching identity information for digital goods or services of exceptional value.

Reevaluate Identity Checks

Merchants relying on automated identity checks to validate name and address information should carefully review rules and policies that approve orders where identity information matches and understand the extent to which they may be vulnerable to large-scale attacks where all identity information matches for a significant volume of orders.

Merchants operating in the digital goods and services industries are especially vulnerable to emerging attacks with this characteristic because they are not shipping goods to an address and therefore criminals need not have any link to the address provided to benefit from the transaction.

Ask the question: "If a criminal has a full identity as a result of the Equifax data breach and passes our identity checks, then what other controls are in place to detect the attack?"

If there are no other controls in place that can reasonably be expected to stop a large-scale attack with this characteristic, then the merchant is exceptionally vulnerable to a high-scale clean order attack vector driven by the Equifax data breach. If this vulnerability is found, it is essential to develop compensating controls that can identify such an attack.

Perform BIN Analysis

The new account fraud attack vector will expose specific vulnerabilities at specific issuers. Therefore, the incidence of new account fraud is likely to be highly correlated with the card BIN, which represents the card issuer.

To identify issuers that might be vulnerable to this attack vector, the following metrics should be calculated and reviewed daily and weekly:

1. Growth in order volume from a specific BIN, both in dollar terms and as a percentage of total orders.

2. Growth in chargeback activity both in in dollar terms and as a percentage of total sales for a specific BIN, and growth in percentage of chargeback transactions attributable to a specific BIN as a percentage of total chargeback transactions.

3. Growth in other risk factors linked with a specific BIN. For example, an increase in card decline rate associated with a specific BIN could be a leading indicator of an attack focused on that BIN.

We believe that BIN analysis will become a crucial tool for merchants to rapidly detect and react to new account fraud attacks based on the hypothesis that such attacks will result from exploitation of issuer-specific vulnerabilities.

Consider Additional Authentication Technologies

Consider where it might make sense to deploy additional authentication technologies that are difficult for the criminals to deploy at scale.

For example, if a criminal provides the phone number belonging to the identity they stole, they will not be able to answer that phone if the merchant calls to verify the order.

If the criminal obtains a phone number and provides it to the merchant, then the merchant can attempt to verify the ownership of that phone number and may discover that the owner of the number does not match the rest of the identity or that the number is a virtual or disposable number.

While calling customers is a verification method of last resort, it remains an effective authentication method in the face of attacks driven by data stolen from Equifax if the verification process is implemented thoughtfully, carefully, and competently.

With the stolen Equifax data, it may become easier for criminals to open phone numbers with established telephony providers that match the stolen identity, and merchants should be aware of this case. However, we believe it would be difficult enough to execute this task at scale such that criminals would obtain such numbers only to commit extremely high- value crimes. Therefore, merchants offering very high-value goods or services should consider this option more so than merchants offering less valuable goods and services. Obtaining a phone number with matching identity characteristics only makes sense for a single high-value transaction and likely cannot be scaled to support a large number of relatively less expensive transactions unless a particular telephony provider is shown to have exceptionally weak risk management practices, making it easy for criminals to purchase large quantities of phone numbers that

match stolen identities. Merchants may want to perform an analysis similar to that described for BINs but focus on telephony provider identities to watch for specific providers correlated with fraud.

Protect Established Customers

It is remarkable how few merchants have features in place to approve orders from established good customers. As a consequence of this shortcoming, orders from good customers are rejected because they meet certain risk criteria, but they should be automatically accepted if the apparently risky criteria haven't changed over time and the customer has established themselves as being legitimate.

Furthermore, the manual review team is overburdened with the need to continually re-review orders from established customers. The need to keep checking orders from the same customers repeatedly takes away time and resources that should be dedicated to studying orders from new customers. At no time is this problem more evident than during the holiday season, when order volumes vastly exceed the merchant's capacity for manual review.

In an era of increased attack velocity, it becomes ever more important to develop an effective strategy for clearing orders from known good customers so that all resources can be dedicated to assessing the risk of orders from potential customers with no history.

Prevent Redirection

In the case of new account fraud, criminals may try to construct orders where the billing address is the same as the shipping address to avoid detection by rules that look for a mismatch. Then, criminals may try to change the delivery address with the shipping company after the order has been placed.

This attack vector has been frequently exploited in the past and we have always recommended that redirection not be allowed. The elevated risks posed by the Equifax data breach underscore the importance of ensuring that shipping partners do not allow packages to be redirected from the original ship-to address approved when the order was placed. Merchants should provide legitimate customers with alternative methods for changing delivery addresses after an order has been placed.

Deploy Extensive Reporting and Monitoring

Too many merchants put payment operations (including risk management) on auto-pilot.

Large-scale attacks with devastating consequences can only occur when nobody is paying attention to the clues, and there are always clues.

Given that 145 million full identities have been compromised and that criminals must be working to devise attack vectors that leverage this data for large-scale automated attacks, it is unacceptable to ignore key indicators of emerging fraud attacks.

In this section, we have provided a range of actions that merchants can take to evaluate their defense postures and close vulnerabilities, but in this environment, it is dangerous to assume that existing controls and processes are successfully stopping attacks.

It is therefore essential for merchants to deploy reporting and monitoring solutions that provide quantifiable insights into the performance of risk management systems and processes, measurements of actual fraud performance, and leading indicators of fraud attacks.

Reporting and monitoring that measures actual fraud performance is the only control that can reliably be depended upon to protect merchants from truly catastrophic fraud attacks.

How Curaxian Can Help

Since 2006, Curaxian has been a trusted partner to more than 75 leading merchants and has consistently helped high-risk merchants achieve low fraud rates in the face of exceptionally sophisticated fraud attacks. Our proven methods help merchants navigate unprecedented risk. We offer three solutions that are relevant to merchants wanting to ensure success in the post-Equifax breach environment.

Curaxian Analytics – Reporting and Monitoring

Our reporting and monitoring solutions help merchants detect fraud attacks being missed by current controls and processes. As criminals weaponize the Equifax data to develop new automated attack vectors that scale to take advantage of 145 million new identities, it's more critical than ever for merchants to identify exploitation of vulnerabilities. What worked in the past may not continue to work in the future, because the Equifax data gives criminals new capabilities.

Since 2011, our solutions have consistently and repeatedly helped leading merchants identify new attacks in their early stages, and none of our clients have ever been blindsided by an undetected large-scale attack while using our software and services.

It's easy to get started: We connect directly to your acquirer, so you don't need to do any work to set up the service.

Manual Review Training

We offer the most comprehensive manual review training program in the industry. Merchants who use our manual review process have achieved consistently low fraud rates in the face of extraordinarily sophisticated fraud attacks while maintaining reasonable order review rates and manual review staffing levels, and protecting orders from legitimate customers.

Our manual review package includes the following features:

1. Detailed policies and processes for making the right decisions,
2. A decision-making flowchart that takes ambiguity out of the decision-making process,
3. An on-site training session to train agents on the material and ensure mastery, and
4. Follow-up support to ensure continued success.

Our manual review package arms merchants with processes, policies, criteria, and methods that ensure consistent decision-making over time and across agents, and is also an invaluable tool for on-boarding new agents and ensuring continued consistency through staffing changes or while ramping up for holiday volumes.

Risk Audits and Strategy Development

Before the Equifax breach, many merchants were already pushed beyond the breaking point by advanced attack technologies that make it nearly impossible to detect fraudulent orders using currently available tools and techniques.

We expect the weaponization of the Equifax data and the creation of derivative data sets to fuel vastly more sophisticated automated attacks with flawless and fully verifiable identity data.

We have a strong understanding of the latest attack trends and merchant vulnerabilities, and we know how to fix those vulnerabilities. We also understand how criminals are likely to modify their attack vectors to get the most benefit from this data set and we know how those modifications will intersect with merchant vulnerabilities to create new opportunities for the criminals and threats for merchants.

With this know-how, we are uniquely qualified to assess your current control environment and identify modifications necessary to ensure protection against new forms of attack arising from the capabilities that criminals will develop to make use of the Equifax data.

A typical audit and strategy development engagement has three main parts:

1. We assess your current fraud rules, processes, policies, and technologies, then
2. We identify gaps in your control structure that criminals might exploit with their new capabilities, then
3. We recommend changes to fraud rules, processes, policies, and technologies to ensure those gaps are closed.

The outcome of an audit and strategy development engagement is a better risk strategy that provides protection from the new attack vectors we anticipate seeing as soon as the 2017 holiday season.

How Can We Help?

Contact Mitch Muroff (mitch@curaxian.com) to discuss.

Summary

In summary, as a result of the Equifax data breach, we expect to see three emerging trends in criminal attack vectors that will affect e-commerce merchants.

1. Greater use of new credit card numbers opened by criminals using identities stolen from victims of the Equifax breach. Merchants should evaluate current controls, processes, and policies to ensure they can detect attacks with this characteristic, particularly those involving high-value purchases.

2. Data provided with orders will become cleaner as criminals use the stolen identity data on 145 million American consumers to provide names and addresses that perfectly match the data in databases used for order verification. Merchants should evaluate current controls, processes, and policies to ensure they are not overly reliant on rules or policies that check these data elements and verify that other checks are in place to catch orders from criminals that have verified names and addresses.

3. Criminals will be emboldened to respond to verification calls from merchants with Social Security numbers, dates of birth, and driver's license numbers stolen from Equifax. With this data, the criminals may be able to gain access to additional data sources such as prior addresses and entire credit histories of the identity victims to further prepare for merchant verification calls. Merchants need to rethink the questions they ask during verification calls and the methods they use for determining how those calls are conducted (i.e., what numbers are called, how those numbers are verified, and how inbound calls are treated) to ensure they are speaking with the actual cardholder and not the criminal when calling to verify an order or performing other verification functions.

About

Curaxian

Curaxian helps merchants and processors solve risk and payment related challenges and develop best-in-class risk and payment operations. Since 2006, we've developed solutions for more than 75 leading merchants representing more than $400 billion in annual transaction volume.

Curaxian's software, Curaxian Analytics, leverages merchants' payment data to optimize revenue growth, customer experience, processing costs and fraud prevention. It was recognized by Finovate and the PYMNTS Innovation Award and was voted one of the top 3 most important innovations by the Merchant Risk Council's METAwards.

Mitch Muroff

Mitch Muroff is the founder of Curaxian. He has 25+ years of payment industry experience helping companies develop payment strategies to increase profitability and manage fraud risk.

As Lead Program Manager at Microsoft, Mitch launched the global payments infrastructure for shop.microsoft.com. He later managed transaction risk for a marketplace with 10M customers at an AT&T-acquired startup. As Yahoo's Electronic Payments & Risk Management Director, he drove payment strategy and managed fraud risk for 30 lines of business worldwide.

He helped Edgar, Dunn & Company extend its practice into merchant payments then founded Curaxian to focus on e-commerce. Curaxian has supported 50+ merchants and payment processors with $400B+ in annual transaction volume.

Mitch's expertise includes fraud risk management, recurring billing, product design, competitive strategy, reporting/metrics, due diligence, vendor selection, and recruiting. His fraud risk management experience includes analytics, incident response, audits/assessments, manual review, training, and managed services.

Mitch is a founding member of the Merchant Risk Council's Benchmarking committee and a regular speaker at industry conferences. He has published two articles about sophisticated fraud attacks and has been quoted by The WSJ, Nilson Report and PayPers.

He has an MBA from the University of Washington and a BA in Finance and Economics from the University of Western Ontario.

His interests include meditation, cuisine and kitesurfing.

Sources

[1, 2, 3] https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/

[4] https://www.equifaxsecurity2017.com/2017/10/02/equifax-announces-cybersecurity-firm-concluded-forensic-investigation-cybersecurity-incident/

[5] https://www.pymnts.com/global-fraud-index/