Rocio Baeza - CyberSecurityBase Response to Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning

July 1, 2021

Thank you for soliciting information and comment on Financial Institutions Use of Artificial Intelligence and Machine Learning.

This response is structured to provide information on my professional work experience, address question #17 in the RFI, focusing on the risk that consumers will face with increased adoption of AI and ML, and issue actionable recommendations for agencies reviewing the RFI responses.

My name is Rocio Baeza. I am based in Chicago, a working professional, mom of 2, spouse, and data privacy advocate. I am the CEO and Founder of CyberSecurityBase, a consultancy that helps Legal and Compliance Executives with information security and compliance initiatives. The team specializes in the online small-dollar lending space. This may be in the form of an outsourced security and compliance team, customized development and implementation of policy and procedures driven by consumer protection laws and regulations. After graduating with a B.A. in Mathematics from the University of Chicago, I started my professional career at CashNetUSA. CashNetUSA was a rising payday lender that grew into what is now known as Enova International, a publicly traded company with an international presence in the financial services and data analytics space. While employed at Enova, I supported recognizable brands, including Cash America, NetCredit, QuickQuid, Pounds to Pocket, and Enova Decisions. Since then, I have supported clients on a consultant basis, spoken at professional trade events, and voiced concerns with the current state of the cybersecurity field to regulators. This includes providing commentary to the proposed changes to the GLBA's Safeguards Rule, participating in the FTC's Safeguards Rule Virtual Workshop in July 2020, and in 2020, joined as members of the the Online Lenders Alliance to engage with industry leaders and regulators in conversations of information security and compliance to federal consumer protection laws. My professional background provides me with a unique perspective that I seek to share, to educate regulators, influence regulation and guidance from agencies that regulate the online lending industry, with the end goal of protecting the everyday American consumer from negative impact resulting from inadequate protection of personal information processed by the financial services industry.

For purposes of this response, machine learning refers to the search for patterns in massive amounts of data[1]and artificial intelligence is intelligence displayed by machines that process

[1]https://www.technologyreview.com/2018/11/17/103781/what-is-machine-learning-we-drew-you-another-flowchart/

massive amounts of data. The result of AI and ML is problem-solving that mimics natural problem-solving from humans, but at a larger scale.

Question 17: To the extent not already discussed, please identify any benefits or risks to financial institutions' customers or prospective customers from the use of AI by those financial institutions. Please provide any suggestions on how to maximize benefits or address any identified risks.

When a financial institution uses AI on their customers or prospective customers, there is both a benefit and a risk. Several benefits have been identified in the *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning* document. I trust that financial institutions and trade associations that respond to this RFI will further elaborate on the benefits. My goal is to provide information to agencies[2] as they seek to provide further guidance to financial institutions to ensure safe and sound use of AI and in compliance with consumer protection laws and regulations. The information provided in this response is set to serve as a voice for the everyday American consumer that may not understand what is at stake, if the adoption of AI and ML is not properly regulated.

A financial institution's use of AI will increase the risks to the everyday American consumer. There is one risk that is most concerning to me, and worthy of your consideration in this RFI process: the risk of identity theft. Identity theft is a real risk that exists in the financial services industry, because of the nature of data that is collected by financial institutions. This includes personally identifiable information (such as name, SSN), contact information (such as postal address, email address, IP address), employment information (such as employer, position, wages), and payment instruments (such as bank account numbers, credit card numbers). An SSN with another piece of identifying information is usually sufficient for one individual to successfully assume the identity of another individual. *For this reason, it is imperative that the reader carefully examine the information shared in this RFI response, and consider the recommendations included here.*

Customers and Prospective Customers of Financial Institutions Using AI Are At Risk of Identity Theft because of the perfect storm that we are currently facing. Financial institutions have increased the adoption of technology to provide products and services to the everyday consumer. This has resulted in new products and services not available 10 years ago. Most notably, being able to apply for credit from a smartphone and receive funds on the same or next day. Financial institutions have been able to reach this point, in partnership with service providers, including lead providers, credit reporting agencies, cloud service providers, payment companies, online banking systems, and data warehouse providers, to name a few. The pandemic caused by COVID-19 forced a rapid digital expansion for both consumers and

[2]Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency

financial institutions. At the same time, the cybersecurity field is still in its infancy, it continues to face a shortage of skilled cybersecurity professionals, leaving many rising FinTechs without access to quality cybersecurity talent. This has and continues to create a challenge for FinTechs, as business leaders struggle to understand and manage cybersecurity risks. This struggle in understanding and managing cybersecurity risk is in large part, due to the intangible nature of the field. Cybersecurity is a field that focuses on protecting data that is in a virtual form and is manifested in a physical form through the display of a computer screen or paper print out.

A financial institution's use of AI will increase the risk of identity theft for the everyday American consumer, because it will expand the digital footprint of data. This expanded digital footprint creates a larger attack surface, compounding the issues because of the factors described above.

Simply put, identity theft can lead to a number of consequences for a victim:

- loss of personal finances
- loss of time
- degradation of one's personal well being
- loss in personal freedom and liberties

Let us examine the specific risks that the everyday American consumer will face, as a result of the unregulated use of AI and ML by financial institutions.

*Risk 1: Customers and Prospective Customers of Financial Institutions Using AI Are At Risk of Identity Theft and Face **Losing Personal Finances** to Address and Resolve Cases of Identity Theft*

Victims of identity theft are required to spend money to contain and clean up any damage. These victims often face fraudulent purchases and applications for credit made by the criminal. These victims may need to spend money for a number of services, including to cover the cost of identity monitoring services (to assess the extent of the damage), the cost of retaining an identity theft recovery specialist or lawyer (to report to authorities and businesses), and the cost of fees resulting from fraudulent transactions (fees that grow until the transaction is flagged as fraudulent). *In some cases, this may also include temporary or permanent loss of money in savings or checking accounts, loss in unemployment insurance benefits, or loss in retirement savings/income.*

*Risk 2: Customers and Prospective Customers of Financial Institutions Using AI Are At Risk of Identity Theft and Face **Losing Time** to Address and Resolve Cases of Identity Theft*

Victims of identity theft are required to spend time to assess the damage, contain the situation, resolve the situation, and monitor the situation for new damage. These victims spend time calling credit reporting agencies, banks, credit card companies, and businesses to gather information on fraudulent transactions, file a report with business and police, place a credit

freeze, and follow additional processes to ensure that transactions are classified as fraudulent. *In some cases, victimes may also need to spend time working with law enforcement agencies and a lawyer to address any criminal activity performed by the criminal, in the name of the victim of identity theft.*

Risk 3: *Customers and Prospective Customers of Financial Institutions Using AI Are At Risk of Identity Theft and Face A* ***Degradation of their Own Personal Well Being*** *to Address and Resolve Cases of Identity Theft*

Victims of identity theft often face stress, frustration, and anguish that if left unmanaged, can lead to a mental and emotional state that can start to degrade their personal well being. This may be experienced over the course of assessing the situation, containing the situation, and trying to resolve the situation. This is a subjective area and will vary from individual to individual. However, the degradation of an individual's own personal well being impacts their quality of life, and cannot be overlooked. This may materialize in stress, frustration, or anguish because of:

- the victim's inability to secure a dream job that runs a background check that includes activity related to the case of identity theft
- the victims inability to secure an apartment, mortgage, or finance a car or student loan because of bad credit created by the identity theft
- *the victims inability to travel overseas, because of criminal activity performed by a criminal, in the name of the identity theft victim*

Risk 4: Customers and Prospective Customers of Financial Institutions Using AI Are At Risk of Identity Theft and Face ***Losing Their Personal Freedom and Liberties*** *Because of Identity Theft*

There are victims of identity theft that face losing their personal freedom and liberties because of a criminal that commits a crime in the name of the identity theft. A personal relative came to learn that someone assumed their identity, committed a crime, was charged with the crime, and has an active arrest warrant. This relative has spent time and money to react to this situation. This relative has also changed how they carry out their day to day activities, to minimize any contact with law enforcement officials. They know that a wellness check, traffic violation, employment background check, or air travel will lead to a chain of events once law enforcement learns about the active arrest warrant on his record. This already happened on a return trip back from vacation. It was through the grace of God that my relative was able to return home that day to his family. Let me emphasize that this relative has changed how they carry out their day to day activities, to ensure they get to return home each day. This worries me deeply because it can happen to anyone, to me, my son, my daughter, my husband, my father, and mother.

In summary, financial institutions' use of AI will increase the risks to their customers and prospective customers. The financial institutions' use of AI will increase the risks of identity theft, forcing victims to spend time, money, and in some cases, risk their personal well being or personal freedoms while they address the case of identity theft.

It is important to underscore that these risks not only apply to customers and prospective customers of financial institutions, but also non customers and non prospective customers. Financial institutions see value in data about individuals to understand patterns and behavior. Through the course of everyday business, financial institutions are gathering, storing, and in some cases, analyzing data of non customers and non prospective customers, because the data is available. In the online lending industry, this is a common practice in the case of data vendors and lead providers.

In the case of data vendors, they aggregate significant amounts of data about the everyday American, oftentimes without the individual's knowledge or consent. This may include credit transactions, shopping history, digital footprint, geolocation data, email account usage, and media consumption history. In this case, the everyday American is oftentimes not aware of this data collection, let alone that data about them is shared and sold by data vendors to any organization that is interested in engaging in a data study or willing to purchase that data.

In the case of lead providers, they aggregate significant amounts of data about individuals that have expressed interest in an online loan. The lead provider presents an application form online for the individual to complete and once submitted, it is shared with a *vast network* of financial institutions that have seconds to decide whether to purchase the lead or not. In this case, these individuals are oftentimes not aware of this data sharing and data selling ecosystem.

The data sharing and data selling ecosystem is only understood by very few practitioners in the industry. This data ecosystem has created so much value for the industry. However, the industry, consumers and regulators are unable to assess the risk that this is creating for the everyday American consumer, because of the digital nature of this data.

My hope is that I have articulated the current situation in a clear way, as to demonstrate that financial institutions' use of AI and ML impacts all individuals and requires careful examination from regulatory bodies and agencies.

If left unregulated, a financial institution's use of AI will increase the risks to the everyday American consumer.

Recommendations

There are a number of measures that financial institutions can take, to minimize the risk of identity theft for the everyday American consumer. At the end of the day, these measures are related to cybersecurity and information security. There are financial institutions that have the budget and personnel to stand up a world class cybersecurity program. Unfortunately, cybersecurity is an industry that is still in its infancy. This means that not all financial institutions have access to skilled cybersecurity professionals that can implement an effective cybersecurity program that protects the IT systems of the financial institution AND personal information of their

customer and prospective customers. With this in mind, I propose the following recommendations for your consideration.

Recommendation #1: Advance the proposed changes to the GLBA Safeguards Rule

The GLBA's Safeguards Rule is out of date and does not take into account the increased adoption in technology by both financial institutions and consumers. As it is written, it sets an unreasonable expectation that documentation addressing the top-level elements is sufficient to satisfy the letter and the spirit of the Safeguards Rule. This has become apparent to me, *only after* practicing as a cybersecurity professional for the last 10 years, supporting FinTechs for almost 15 years, having served as a product manager at a rising FinTech (Enova International) working alongside software development teams, continuing to work with software development teams when supporting clients, and increasingly engaging with Legal and Compliance Executives to support information security and compliance initiatives.

As written, the Safeguards Rule provides Financial Institutions with flexibility on meeting the requirements. However, with the increased adoption of technology, this flexibility is cause for concern for financial institutions that do not have access to cybersecurity expertise. The anticipated adoption of AI by financial institutions will only worsen the problem here.

Recommendation #2: Retain specific elements in the proposed changes to the GLBA Safeguards Rule

Upon finalizing the changes to the GLBA Safeguards Rule, consider retaining the proposed changes around:

- Annually requiring a written report to the board or governing body, to include information on the overall status of the information security program, compliance with the rule, and managing information security risks
    - This measure will help elevate security risks as business risks, and force the cybersecurity industry to improve how it communicates cybersecurity risk to executives
- Implementing policy and procedures that includes providing security awareness training that is updated to reflect risks identified by the risk assessment
    - This measure will help break the current cycle of financial institutions engaging general elearning providers, to check the box, but not moving the needle in helping the financial institution effectively manage information security risks
    - This measure will also help standardize the hierarchy for an effective information security program (i.e. requirements set at the policy level, how to direction set at the process level, education being delivered via security awareness training, audit to provide compliance assurance, and risk assessment outputs to inform changes to policy, process, or training)

- Basing the information security program on a risk assessment that is written, and includes capturing response and decisions on identified risks (just to name a few of the proposed components)
    - This measure sets a clear expectation that the risk assessment is a formal exercise that is carried out in a methodical way to provide information to the financial institution that can be used to mature the information security program and better manage cybersecurity risk

Recommendation #3: Update the proposed changes to the GLBA Safeguards Rule to require foundational elements that are critical for an information security program to be effective

The proposed changes to the GLBA Safeguards Rule are missing foundational elements that are critical for the effective management of information security risks. These are the data inventory, 3rd party inventory, IT system inventory, and data flow diagram. These are foundational elements that establish the scope of what an information security program aims to protect.[3]

Traditionally, financial services have operated in a well-defined space that is guarded with physical controls. At a minimum, this includes a security guard, separation between tellers and consumers, a vault, and alarm systems protecting the physical building housing a financial institution. Today, financial services are operating online, with systems managed in-house, by 3rd party vendors, and in some cases, by business professionals. This decentralized IT infrastructure expands the digital footprint of consumer data. This quickly shifts us from having a dedicated team of IT professionals to manage an IT system to having all levels of a financial institution managing various IT systems, in some cases, without formal training for securing the IT systems under their watch.

Recommendation #4: Level the playing field between Financial Institutions and service providers with corporate accountability in the event of a security incident resulting from action by the service provider

In supporting FinTechs with building an information security program, it is common to see Financial Institutions struggle to get service providers to agree to security terms in a contractual agreement. In the last 5 years, there has been a growing trend for service providers to provide SaaS-based services, and require financial institutions to agree to the standard Terms of Use that excuse themselves from any responsibility of a security incident, even if caused by a member of their team or due to negligence. Not being a lawyer, I don't know what needs to be done to ensure a leveled playing field for both the financial institution and service provider. But

[3] See pg 3 of my response to the Postponement of Public Workshop Related to Proposed Changes to the Safeguards Rule on https://www.regulations.gov/document/FTC-2020-0038-0001/comment

my contribution will be to raise concern on this matter and trust that through this RFI process, Legal experts can offer options for a solution.

Recommendation #5: Establish a national organization for cybersecurity professionals to ensure consistent education and professional accountability of professional services

The cybersecurity industry is full of professionals with a wide range of technical aptitude, experience, approaches, and methodologies. This presents excellent opportunities for professionals eager to learn and contribute. However, it also presents excellent opportunities for individuals to perform a cybersecurity risk assessment, audit, or gap assessment that is ineffective and inconsistent, because there is no governing body that sets the standard for all cybersecurity professionals.

Recommendation #6: Engage with cybersecurity professionals to develop resources to educate auditors, investigators tasked with enforcing consumer protection laws and regulations

The cybersecurity field is highly specialized. Investing in educating auditors, and investigators tasked with enforcing consumer protection laws and regulations like GLBA's Safeguards Rule.

In closing, I appreciate the invitation to provide comments on Financial Institutions' use of AI and ML, as this is an important matter. If left unregulated, a financial institution's use of AI will increase the risks to the everyday American consumer. Please consider this information and these recommendations as you collaborate with your teams to decide on appropriate guidance to financial institutions to ensure safe and sound use of AI and in compliance with consumer protection laws and regulations.

Sincerely,
Rocio Baeza
CEO and Founder
CyberSecurityBase
rocio@cybersecuritybase.com

You are invited to view a supplementary video recording on this matter at:
https://cybersecuritybase.com/AI