"The Future of Identity in Financial Services: Threats, Challenges, and Opportunities"

Testimony of

Valerie Abend
Managing Director
Accenture

Before the

Task Force on Artificial Intelligence
Committee on Financial Services
U.S. House of Representatives

September 12, 2019

Chairman Foster, Ranking Member Hill, and members of the Task Force, my name is Valerie Abend and I am a Managing Director with Accenture, where I lead the North America Financial Services Security practice, and serve as the Global Cyber Policy & Regulatory Lead. On behalf of all my colleagues at Accenture, a leading global professional services and technology company, serving 95 of the Fortune 100 and 75 percent of the Fortune 500, thank you for the opportunity to appear before the Task Force to discuss cyber threats and how innovations in digital identity and access management are improving financial institutions' and customers' ability to mitigate cyber attacks, enhance privacy, and ensure trust in financial transactions, and what more needs to be done. My comments today will cover three areas:

1. The increasing volume and sophistication of cyber threats that specifically focus on credential theft and exploit privileged access;
2. The significant advances in digital identity systems to combat fraud and provide true needs-based access, while also enhancing customer experience and privacy; and
3. How artificial intelligence is being used to manage cyber risk both for internal access within financial institutions and for customers.

Credential Theft and Privileged Access

First, let me address the increased volume of cyber threats, particularly credential theft and the growing trend of bad actors exploiting privileged access. In our recently published paper entitled, "Future Cyber Threats: Extreme but Plausible Threat Scenarios in Financial Services,"[1]

[1] https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf#zoom=50

which I have provided to the Task Force for inclusion in the hearing record, we explore how current cyber threats will be increasingly directed across multiple institutions and third parties simultaneously, potentially causing extreme impacts. The five key themes in the paper are: 1) credential and identity theft, 2) data theft and manipulation, 3) destructive and disruptive malware, 4) emerging technologies, and 5) disinformation. While my remarks before the Task Force today focus largely on credential and identity theft, the paper describes how all five threat themes may come together in the future to impact financial services. Credential theft was our first theme because this is how most attackers initiate a financial institution breach.

Phishing and spear phishing have been problems for more than a decade because it works. Malicious cyber actors can cheaply target large volumes of people and entice users to click on links or open attachments that imbed malicious software that enables the attacker to scrape a user's log in information. For attackers, it also helps that people put vast amounts of information about themselves online, making it even easier for bad guys to identify specific targets and construct a social engineering campaign to steal a particular individual's login credentials.

Securing credentials is a key challenge for both retail and wholesale financial services.

Today, sophisticated attackers don't just go after one bank, they go after the end to end process, which includes the customers, deposit institutions, clearing banks and central banks. They identify vulnerabilities in the processes, leverage countries with weak money laundering enforcement, and target specific employees and third-party employees' credentials. We call these multi-party attacks and they are becoming more common.

One well-known example of this is the 2016 cyber heist from the Bangladesh Central Bank, where attackers successfully stole more than $81 million. The attack started in 2015, when

attackers set up seemingly legitimate bank accounts, using fraudulent identities at several institutions. They then targeted the specific identities of employees at the Central Bank who were part of the wholesale payment transactions value chain. The attackers knew the systems they had to effect and the credentials they needed to control to carry out the attack unnoticed and transfer stolen funds to accounts they set up with fake identities. This was four years ago, and adversaries are continuously learning.

Advances in Digital Identity

Fortunately, while the bad guys have gotten smarter, the good guys have too. Financial institutions are making investments to thwart these types of attacks and manage risks more effectively. These include people, process and technology. Cyber threat intelligence teams both internally within institutions, along with external providers, are helping companies build more effective defenses. Advanced security operations centers are enabling companies to identify attacks sooner and take mitigation measures more quickly. Robust awareness and training initiatives are helping employees better understand social engineering attacks and know what to look out for. Information sharing about threats and vulnerabilities is also more robust than ever before through the Financial Services Information Sharing and Analysis Center (FS-ISAC). And to the topic of today's hearing, the financial services industry is an early adopter of digital identity innovations. These innovations provide better risk engines to make it harder for fraudsters to gain access to customer accounts while enhancing customer experiences.

Consumers expect seamless and easy to navigate online services, and institutions are working to meet that demand by growing their online products and services. Online and mobile banking are

now table stakes in a digital economy. To stand these operations up quickly and efficiently, commercial entities initially rolled out platforms that relied heavily on customers setting passwords and answering security questions to authenticate their identities online. Unfortunately, today a large percentage of Americans' names, addresses, birthdays, social security numbers, and other information, used by fraudsters and state-based cyber actors to guess passwords and answers to personal questions, is available on the dark web. The days of the username, password, and security questions as tools to manage risk are numbered.

This is where the concept of customer digital identity comes in.

Increasingly, financial institutions are implementing an array of products and services - such as biometrics, behavioral analytics, and multi-factor authentication - to help them make real-time, risk-based decisions about whether to authenticate a customer, approve a transaction, and what limits to set around a transaction.

Because of these new tools and techniques, individuals can be digitally authenticated anywhere in the world, in real-time. For example, I was recently traveling overseas and could log into my banking app on my mobile device using my thumbprint. The bank would have used the identifier from the phone, my location information, and many other factors to determine if I was actually Valerie Abend. If, at the time, the bank noticed anomalous activity in my account, its algorithms would have decided whether and what additional information it needed from me to provide me access to my account. Of course, as with any new process and technology in this highly-interconnected digital age, there could be other implications, and in this case, depending on the types of information that is gathered or that I share with the institution, there could be privacy implications for an effective risk management approach. Ultimately, the digital identity ecosystem I've outlined above will not just be limited to financial services but will also spread to

other parts of the economy. That is why Accenture believes Congress must pass a national privacy law that provides consumers with rights for transparency, control, access, correction and deletion with respect to their data. A robust and secure digital identity ecosystem depends on privacy to build trust and will not thrive without it.

The Role of Emerging Technologies in Managing Risk

One of the most ubiquitous new technologies being discussed today is artificial intelligence (AI). Not a day goes by without some mention of the promise of AI in all sorts of business settings, and cybersecurity is no different. The unfortunate reality is that bad guys will use AI as part of cyber attacks. While that can be scary, it should also give us some comfort to know that agile and forward leaning organizations will also leverage AI to defend themselves. AI will enable automated detection, response, and mitigation in security operations centers, intercepting attacks faster than humans can today, and stopping suspicious events before they become actual, harmful incidents.

AI is also increasingly being used to help ensure needs-based access management internally to financial institutions. Within many financial institutions there is a significant amount of attention and resources paid to identity and access management. Identity access and management includes policies, technologies, and processes that are meant to ensure that customers, employees, and even contractors only have access to systems and information necessary to perform their transactions or do their job.

Most institutions use a principle called role-based access control (RBAC) to manage their identity and access management. For example, when an employee starts her job at an

institution, she needs access to certain systems. We call this day-1 access—things like email, human resource systems to select and receive health benefits, and payroll systems so she can get paid. All of that day-1 access is put into something called a role. In addition, the new employee likely is joining a particular group within that institution and that means she probably needs access to certain applications and datasets to do her job. That's another role. She likely needs access to more than just one role because her job requires her to work with information across different groups at the institution. Let's say she does a great job and gets promoted. She even gets transferred to a new group and gets additional roles. Over time, she accumulates a lot of roles with the access that goes well beyond what she needs to do her job at any one time. Some of these access rights might include privileged access to sensitive data or systems including the ability to not just see information and systems but to copy them or make changes. Let's take a step back now and multiply this one woman's access across thousands of people and thousands of systems inside a single institution and you have a very complex risk management challenge. Today this process is manual, inefficient, and hard to maintain in alignment with current risk management principles.

This is why institutions are starting to use AI to have a more accurate, real-time understanding of access enables supervisors to make better access management decisions. This is really important. Most breaches involve some type of gap in the identity access and management process—either from the customer or employee or both. Innovative approaches, such as AI, can deal with complex and highly vulnerable processes and will increasingly be essential to thwarting cyber attacks.

From a customer perspective, we are helping to spearhead important innovations using emerging technologies such as blockchain, biometrics, and encryption, to enable large numbers of

customers to verifiably identify themselves with an audit trail to their bank, while still being in control of their own identities in a virtual world. The best example is the ID2020 project. As a Founding Alliance Partner of the public/private alliance called ID2020, Accenture built the decentralized ID prototype and launched it in June 2017. This blockchain identification system was designed to provide reliable digital identity to refugees so they can confidently receive government services, and validate their identity to employers, schools, and other service providers. Additionally, it gives users control over who has access to their information and for what period of time. As innovations like this progress, it is likely they will leverage AI to further enhance both risk management scoring of customer identities and their customer experience.

Imagine a world where we broadly apply these kinds of techniques across financial services. Americans will have the opportunity to exert real control over their data. They would share what they want, when they want, with whom they want. Instead of filling out long application forms, repeating the same information over and over—users can populate those forms with a simple click of the mouse or touch of the thumb, saving millions of hours of time while simultaneously and dramatically increasing security and privacy. Of course, as I noted earlier, new processes and technologies also introduce new challenges. In the case of AI, there are four key areas where we need to manage risk:

1. The security and quality of the data informing the algorithms.

2. The security of the algorithms.

3. The quality and accuracy of the outputs—looking for disparate impact, bias, and malicious compromise or manipulation of data.

4. Effective and responsible AI governance approaches.

Looking forward

There is a lot of work to be done to make these emerging technologies work in favor of customers. From where I and others sit, based on the industry's long history of being heavily regulated and the importance of safety and soundness of the industry, financial institutions are best positioned to leverage these new technologies as early adopters while managing the risks to enhance the financial lives of Americans. The World Economic Forum's January 2018 report, *On the Threshold of a Digital Identity Revolution*, noted that people and legal entities in many countries already leverage documents from financial institutions as a form of identity to gain access to other services. This positions the sector as a prime candidate to act as a trusted identity provider.[2] Proofs of concepts should be encouraged, and their ability to scale should be assessed. Interoperability is essential, as any new tools or techniques should work with not just one company's systems, but also with those in other industries. And financial services should lead the way in moving away from the Social Security number as a key authenticator. The role of the Social Security number has moved well beyond its original intent, giving it unintended power and value that ultimately has made it possible for bad guys to commit a myriad of fraudulent activities. The time has come to find a way to diversify off the Social Security number so that it is no longer a proof of who you are in an online environment.

Broadening and scaling the use of digital identity across the economy will require new levels of cooperation and collaboration between the private and public sectors. This was a key conclusion reached in a white paper, *Building Trusted and Resilient Digital Identity*, recently released by Business Roundtable, a trade association consisting of more than 200 CEOs of leading U.S.

[2] World Economic Forum, *Digital Identity On the Threshold of a Digital Identity Revolution*, January 2018 http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf

companies. The paper, developed under the leadership of Accenture CEO Julie Sweet, made eight recommendations to advance private and public development and use of digital identity, including:

- Reducing our dependency on passwords in favor of more intuitive and secure authentication;
- Increasing customer awareness, digital literacy, and confidence;
- Improving multiple sector participation in a digital identity ecosystem that enables trust in each other's attestations of identity—so users can continue to transact business even when an individual organization's digital identity system has been breached; and
- Ensuring transparency and choice to customers, empowering them with customer rights. A national privacy law would go a long way to achieving this goal.[3]

What does all of this mean for Congress? As this Task Force and Congress as a whole, considers legislation and other avenues in the areas of digital identity and cybersecurity in the financial services sector, I would encourage three things specifically:

- Ensure legislation is truly technology neutral and does not effectively choose winners and losers in the marketplace;
- Pursue policies that will protect and advance innovation, which is essential for our financial institutions to stay a step ahead of the bad guys; and
- Pass a national privacy law, which as I noted earlier, is essential to effective, robust digital identity ecosystem.

[3] Business Roundtable, *Building Trusted and Resilient Digital Identity* July 2019 https://s3.amazonaws.com/brt.org/BRT-DigitalIDReportJuly2019.pdf

Conclusion

In sum, the financial services industry is facing significant changes on the cybersecurity front. Credential theft and abusing privileged access has long been a successful approach for cyber attackers, but their tactics are getting more sophisticated. Fortunately, the industry has made significant advances in digital identity systems to improve user experience, combat fraud, and to limit access to only those who truly need it, which gets at the heart of what our adversaries have used so successfully. And emerging technologies like AI are increasingly needed and becoming part of financial institutions' cyber resilience strategies.

Customers trust financial institutions with vast amounts of their data they are highly regulated. These regulations include cybersecurity supervision, and identity and access management. As such, financial institutions will play an important role as part of the foundation of the digital identity ecosystem today and will help shape its growth in the future. For the sake of the safety and soundness of the financial system, we must create a policy environment that encourages innovation and scaling of digital identity solutions to mitigate cyber attacks, enhance privacy, and help to ensure trust in financial transactions.

Again, I would like to thank the Task Force for the opportunity to discuss these issues today and I look forward to your questions.