Commonwealth Bank
Commonwealth Bank of Australia
ABN 48 123 123 124

Monday 16 March 2020

Committee Secretary
Select Committee on Financial Technology and Regulatory Technology
Department of the Senate
PO Box 6100
Parliament House
CANBERRA ACT 2600

Sent via email: fintech.sen@aph.gov.au

Dear Committee Secretary,

I write with regard to the questions on notice provided by the Senate Select Committee on Financial Technology (**FinTech**) and Regulatory Technology (**RegTech**) on 4 March 2020.

The Commonwealth Bank (**CBA**) is pleased to provide the Committee with additional information as well as to clarify CBA's position in relation to a number of claims made during the Committee's consultations.

1. Competition in financial services

Over the last decade, the level of competition in the Australian financial system has increased, as innovations in technology and changes to regulation have enabled new entrants and smaller competitors to compete effectively.

Customers are benefitting from greater access to new products and services that meet their evolving needs. An example is the home lending market, where there are over 4,000 lending products available with a wide variety of features, offered by 250 financial institutions including neobanks and FinTechs.

In this competitive and innovative market, we are continually considering how we can better serve our existing customers and attract new customers. The ability to deliver new products and services is not solely the domain of either new entrants or incumbents. History has shown that companies, in particular incumbents, need to innovate to meet customer demand and evolve as technology develops. There are many examples of large companies who failed due to their slow response to shifting market demands.

A new emerging market, both domestically and globally, is the availability of micro-investment apps that allow Australian consumers to start investing small, incremental amounts and gradually build a portfolio over time. A number of these products are available locally, of which CBA's CommSec Pocket is one. CommSec Pocket is an extension of our existing CommSec platform, allowing customers to buy and sell a select number of Exchange Traded Funds directly on the stock exchange. Other micro-investing platforms are available with different investment choices and investment structures, and we expect to see further increased competition in this market.

Consumers are the ultimate beneficiaries of the innovation and new product development underway in the Australian financial services industry. As technology advances, we expect innovation and competition for customers to continue to increase over time.

2. CBA's investment in technology, innovation and collaboration

We recognise the benefit that technology offers in delivering the best possible experience for our customers. We are investing $1 billion per annum over five years in our digital services and technology improvements to add further value to our customers as well as keep our systems safe, sound and secure.

This investment in our digital capability and continued development of new products and services is what customers in a competitive market have come to expect. How customers want to bank is changing. That is why businesses – big or small, new or existing – are investing in technology to keep up with the pace of demand. This is a key driver of competition and innovation in financial services today.

CBA is investing in innovation and growth opportunities, including through the launch of X15 Ventures, our new venture building initiative. These opportunities build on the innovation we have undertaken to date, including our Commbank app, awarded #1 mobile banking app in Australia,[1] and our leading data analytics capability.

Last year, we relaunched our CommBank app, which offers our 5.9 million users the first completely personalised and smart digital banking experience, backed by world-leading application of machine learning technology. This year, we plan to make a number of updates to the app, including improved user experience, and also launch new smart features designed to guide customers towards making better financial decisions.

FinTech ecosystem

In understanding the role we have to play in the FinTech ecosystem, on 4 February 2020, we launched X15 Ventures – an Australian technology venture building entity within CBA. X15 Ventures will have its own delivery model, dedicated management team, and be able to access funding from our annual technology investment to provide hands on support to help ventures to scale. In some cases, venture ideas will come from within CBA, in other cases we will identify promising entrepreneurs or ventures external to CBA, and help them to scale through X15.

X15 Ventures is partnering with Microsoft and KPMG High Growth Ventures to deliver new ventures and in turn new products and services for customers. To support the FinTechs and start-ups we work with, Microsoft will bring its platform and engineering capability, while KPMG will provide accounting, tax and advisory services.

X15 Ventures intends to launch more than 25 new ventures over the next five years, beginning with:

- **Home-in** – a virtual home buying concierge that will simplify the complex process of buying a home. Smart technology helps buyers navigate the purchase process more easily, leverage a platform of accredited service providers like conveyancers and utility companies, and reach settlement with certainty.
- **Vonto** – a free app for small business owners that draws data from Xero, Google Analytics, Shopify and other online business tools and presents the data and analytics in one location, allowing users to obtain a holistic view of their business for ease and increased control. To do this, Vonto directly integrates with each third party's application programming interfaces (APIs) and users authenticate for Vonto to receive data.

X15 Ventures will provide CBA with greater ability to seek out more innovative solutions for our customers, and is building a pipeline of ventures and early-stage opportunities initially across four areas:

[1] CommBank Newsroom, *CommBank app leads the pack for the third consecutive year,* 29 June 2019

- **Home and housing** – we are interested in solutions focused on housing and rental affordability and access, managing and optimising a home, and transforming how homes are bought and sold.
- **Modern living, learning and earning** – digitisation of the economy is driving tremendous opportunities, but we recognise it also brings new challenges to employment, financial wellbeing, access and inclusion. We are interested in solutions that tackle everyday hassles, and transform key moments that matter in our lives.
- **Digital and data enabled business** – we are looking for solutions to make it easier to own and manage a business. Business models are transforming in the digital and data economy, and we want to make sure those solutions work for small business, enterprise and Government.
- **Platforms to exchange, record and verify** – we recognise there are lots of problems still to solve in a digitising economy, and in getting ahead of shifts in our economic, social and environmental landscape. We are looking for the next platforms and marketplaces that change the way we create, consume and share goods, services and information.

We encourage FinTechs and start-ups to contact X15 Ventures to discuss opportunities to collaborate.

RegTech ecosystem

We are also focused on delivering better risk, compliance and customer outcomes. The Australian Banking Association is correct in stating there is an industry-wide focus on implementing the Royal Commission recommendations, which is a significant body of work, and we acknowledge that this is necessary, among many other changes, to help restore trust and meet community expectations.

At the same time, we recognise the important role RegTech will play in enabling us to deliver on our regulatory commitments and also understand it will be critical in helping us to digitise, automate and redesign our core risk and compliance processes.

Over the course of the last three years, CBA has moved to accelerate our understanding and adoption of RegTech. Several key initiatives we have undertaken include:

- **Establishing a dedicated RegTech team** – comprised of Emerging Technology and Risk Management experts to work with and accelerate the RegTech ecosystem and help drive RegTech adoption at scale.
- **Collaborating in the RegTech ecosystem** – CBA was the first major bank to become a member of the RegTech Association of Australia (RTA). We have been recognised as a leader in adopting RegTech with impact by the RTA, as the winner of the Regulated Entity of the Year in March 2019.
- **Developed the world's first Global RegTech Alliance** – CBA signed an alliance with ING London, in late 2019, to form the world's first Global RegTech Alliance with the intent of helping to drive better risk, compliance and customer outcomes within the global financial services industry. The Alliance's charter and activities centre on three key areas: intelligence sharing, collaboration and co-development.
- **Executing proof of concepts with RegTechs** – CBA has undertaken a number of proof of concepts with RegTechs, and we are in the process of scaling the deployment of solutions. An example of a recent proof of concept was to understand how we could digitise our end-to-end regulatory change detection and management processes using an integration between Ascent and the Bank's risk management platform. The project, completed in partnership with CBA's risk platform provider, IBM, involved over 230,000 words of regulation interpreted and converted into a series of bite-size, actionable tasks appropriate for the Bank, using artificial intelligence and natural language processing. ASIC participated as an observer in the project.

These initiatives demonstrate our willingness to collaborate and work constructively with members of the RegTech ecosystem to support its growth and development. We will continue

to build our pipeline of solutions, experiments and proof of concepts to identify initiatives that are scalable within our business and deliver better outcomes in terms of risk management and compliance and, most importantly, for our customers.

Cybersecurity

In serving customers at scale, we see how devastating the impacts of fraud, cyber and privacy issues can be for customers. Protecting our customers' data is therefore a responsibility we do not take lightly and, each year, we invest significantly (around $185 million in FY19) in operating and continuously improving our cyber security controls to keep our customers and our systems safe from cyber-criminals.

This is in addition to separate investments we make in continuously improving the security of our online banking applications, and our dedicated fraud monitoring and investigation teams who work 24x7.

Because of the significant amount CBA invests to build a robust cyber and data security capability, we are able to offer our customers a 100% Online Security Guarantee. This means the safety of our customers money is 100% guaranteed, when customers protect how their accounts are accessed and tell us if something is wrong. Sharing log-on credentials puts this guarantee at risk.

In recognising our role and responsibilities within the digital economy, we are engaging with industry, government, academia and individuals on an ongoing basis to enhance cooperation, collaboration and security awareness. We do this by:

- Working closely with domestic and offshore regulators to ensure the bank's cyber controls, policies and processes meet the high standards to which we are held.
- Helping address the nation's cyber skills shortage, including by co-developing content with the University of NSW and helping encourage the development of cyber skills at the high school level through an industry coalition which develops School Cyber Security Challenges with the Australian Computer Society.
- Launching an online portal where organisations can access a free, cyber awareness eLearning module. We also produce a quarterly publication educating businesses about what they can do to protect themselves. We have provided face-to-face education sessions to customers across Australia, targeting approximately 5,000 organisations focused on key threats like business email, password and malware compromise.
- Sharing cyber intelligence with industry, the Australian Cyber Security Centre and other government agencies to help inform how Australian businesses and organisations react to emerging threats.

Since 1 July 2019, we have identified and 'taken down' 267 unique phishing websites. These websites were designed by cyber criminals to appear as authentic CBA websites, but aimed to lure customers into disclosing their bank log-on credentials. Data held by financial institutions is highly sought after by criminal networks – that is why data security is our first priority.

3. Screen scraping and protecting customer data

In its simplest form, the practice of digital data capture (also known as screen scraping) is the process of capturing data displayed on a screen in one application and translating the data so it can be displayed in another application.

For banking customers, this might involve a third party accessing an individual's financial information held within a financial institution's secure website, such as CBA's NetBank. To enable this, the customer has to provide their NetBank username and their password to the third party. The third party will then use the customer's unique username and password to access the customer's account and capture the customer's financial information for use and display in another application.

This provides the third party with the same access rights a customer would have, as they are accessing the customer's account as if they were the customer. This is **not** read-only access. By using this method to access a customer's data, a third party has the log-on credentials required to execute transactions directly on all accounts the customer holds with the bank, be that insurance, banking, and trading accounts.

In relation to submissions the Committee has received from Australian FinTechs, we do not question the intent or practices of most FinTechs who are operating in this manner. However, it remains our firm belief that sharing usernames and passwords is a fundamentally unsafe practice, both in the signals it sends about the importance of these credentials, as well as the storage of these credentials outside the bank's ecosystem.

CBA's primary concern with screen scraping is the security issues it creates. This view is widely held, including by the Basel Committee on Banking Supervision (the Basel Committee), who stated in its *Report on Open Banking and application programming interfaces*, that screen scraping is *"… unsecure for the customer, since the third party maintains the credentials that provide full access to the customer's account".*[2]

The report also acknowledges that:

"Banks, third parties and regulators recognise the security and customer protection risks associated with screen scraping…. Third parties use [this method] to collect and store customer credentials (ie username and password), which could be stolen or misused, including for payment fraud purposes."

"Screen scraping …can undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the customer, data aggregator, and an unauthorised third party that is logging in and extracting sensitive data."

It is, therefore, concerning that third parties encourage customers to share online banking credentials and also communicate that this is a low risk activity.

Risks associated with screen scraping

CBA has more than seven million digitally active customers, who trust us with their financial information, and we take the responsibility of protecting their data very seriously. We continuously review and improve our cyber capabilities to protect our banking environment and most importantly our customers.

CBA's Fraud Analytics team conducted a study on the fraud propensity of customers who had logins via a data aggregator, where we could identify an aggregator. The analysis found that customers with logins via an aggregator are two or more times more likely to experience fraud, a statistically significant result at a 95 per cent confidence interval.

Whilst the study does not attribute cause for the statistical relationship, it does demonstrate a probable correlation between the unsafe banking practice of customers who share log-ons and password credentials with third parties and increased fraud. Behaviours that place customers at greater risk should not be encouraged.

Key risks associated with handing over usernames and passwords, include unauthorised transactions and identify theft. Among other things, it provides:

- full access to all personal and financial information available for the customer, including any superannuation, insurance and CommSec trading accounts regardless of the reason for a party seeking access;
- the ability to transact on bank accounts where two factor authentication is not required; and

[2] Basel Committee on Banking Competition, *Report on open banking and application programming interfaces,* November 2019

- new account set-up functionality.

Screen scraping has been identified as a serious security risk and the European Union (EU) and the United Kingdom are working towards banning the practice. The EU's Second Payments Services Directive (PSD2) was developed to control digital capture practices by requiring banks to create dedicated infrastructure for the sharing of customer data with third party providers and requiring stronger customer authentication, which would prevent screen scraping from occurring.

Recent statistics released by the Office of the Australian Information Commissioner (OAIC) in its *Notifiable Data Breaches Report*[3], for the period July to December 2019, outline that:

- 64 per cent of notified breaches were due to malicious or criminal attacks including cyber incidents of which many have exploited vulnerabilities involving a human factor (such as clicking on a phishing email or disclosing passwords);
- 37 per cent of data breaches notified involved an individual's financial details, such as bank account or credit card numbers; and
- Finance is the second highest reporting sector, notifying 14 per cent of all breaches.

These statistics highlight the ongoing and increasing threat to Australians' personal information and reinforce the importance of protecting customer data, including their log-on credentials.

Customer communications

We communicate with our customers because we have a responsibility to protect the safety of our customers' information, and we can play an important role in customer education and awareness on data and online safety.

We know the security of their data is a concern for customers, who may not be aware of the vulnerability to which they are exposed when providing their log-on credentials to third parties and who seek greater assistance in identifying ways to protect themselves online.

This has been reinforced by independent research commissioned by CBA into Australian consumers' attitudes to online security and their personal data. The consumer research found that:

- 73 per cent agreed it was very important to protect themselves from online fraud and cybercrime and to ensure their passwords are safe and protected.
- 68 per cent were uncomfortable with sharing personal information online but do it anyway.
- 46 per cent are not checking how trustworthy a website is before sharing their personal information online.
- 77 per cent felt they should be doing more to ensure they better protect their online identity.

In our ongoing monitoring of the security of customer accounts, we have identified circumstances where it appears our customers' accounts were accessed by a third party. Where we identify this may be occurring, we warn our customers of the potential risk. We then provide customers the information they need to decide about the steps they can take to protect their security and privacy online.

Our communications are consistent with, and an adjunct to, the annual notifications we are required to provide our customers under the ePayments Code. As a subscriber to the ePayments Code, we are required at least annually to provide a clear, prominent notice summarising passcode security guidelines (clause 8.1). These guidelines must be consistent with the passcode security provisions (clause 12) of the Code, which, amongst other things,

[3] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July-December 2019,* 28 February 2020

include clause 12.2(a), which provides that users must not voluntarily disclose passcodes to anyone, including a family member or friend.

Claims made during the Committee's consultations that our communications are anti-competitive are incorrect. Further, we have responded to enquiries from Raiz Invest in relation to our customer communications and have also offered, in November 2019, to meet with Raiz and discuss options as we move closer to the commencement of Open Banking.

4. Implementation of the Consumer Data Right

As the Committee is aware, the introduction of the Consumer Data Right (CDR) and the development of a secure Open Banking regime in Australia will allow for the secure transfer of consumer information. CBA is a strong supporter of the CDR, the Open Banking regime and the opportunities that will be afforded to customers to share their data in a safe and effective manner.

Importantly, consumers will be in control of their data. Consumers provide informed consent and determine what data to share as well as the purpose(s) for which that data is shared with an accredited entity. Consumers are also able to withdraw consent, and are protected by the CDR privacy safeguards.

In recognition of data security best practice, Open Banking, by design, does not require password sharing. Allowing screen scraping to continue alongside the Open Banking regime will result in effectively 'dual schemes' being in operation, to the detriment of consumers as well as the broader CDR regime. Customers who share data outside the CDR regime may not be aware that they do not have the same consumer and privacy protections.

The CDR is an important Government reform that has the potential to drive significant economic benefit for consumers and the Australian economy. Open Banking will give customers greater control of their data held by banks, enabling the delivery of new services, increasing transparency and delivering more choice and competition among financial products.

CBA's priority in implementing Open Banking, and the New Payments Platform (NPP), is to ensure functionality is introduced in a safe and secure manner without compromising customer protections or the customer experience. Significant investment and programs of work have been undertaken to prepare and build our capability to participate in Open Banking and the NPP. These initiatives are complex and take time to implement reliably. Claims made during the Committee's consultations that delays in the implementation of these initiatives are due to anti-competitive behaviour are incorrect.

Adoption of Open Banking in the United Kingdom was slow in part because consumer trust and awareness were low for the first 12 months. Last year, Deloitte released research showing a similar sentiment in Australia:

- 48 per cent of consumers surveyed would be willing to share their banking transaction information with a major bank;
- Less than 20 per cent would be willing to share that information with a digital bank; and
- Less than 10 per cent with a technology company.[4]

When we demonstrate that Open Banking works, and is secure for consumers, consumers will have more confidence in engaging with new digital technologies. Open Banking is underpinned by a framework, rules and standards that provide consumers with the ability to participate in data sharing without putting their privacy or the security of their data at risk. Accreditation will provide the necessary assurances to consumers and participants that third parties requesting access to financial data meet appropriate privacy and security standards.

[4] Deloitte, *Open Banking: Switch or Stick*, October 2019

As one of the first organisations to be delivering Open Banking for our customers, CBA is committed to building trust in the ecosystem and maximising its benefit for all Australians. We are working towards meeting the revised timeframes for implementing the next phases of Open Banking, including the sharing of consumer data.

Thank you again for the opportunity to provide the Committee with additional information, as well as to clarify our position in relation to a number of claims made during the Committee's consultations.

Should you have additional questions or require further information, do not hesitate to contact me.

Yours sincerely,

Euan Robertson
General Manager
Government, Industry & Sustainability