HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 165 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, May 29, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, May 29, 2019

● (1615)

[*Translation*]

The Vice-Chair (Mr. Matthew Dubé (Beloeil—Chambly, NDP)): Good afternoon, everyone. We will begin the meeting, now that we finally have enough government and opposition members here.

Before I give the floor to our witness, who will be joining us by videoconference, I would like to take a moment to discuss today's proceedings.

Given the time we have already lost, and the uncertainty about this afternoon's schedule due, in part, to the possibility of further votes following the procedural manoeuvres in the House, I would like to make a suggestion.

[*English*]

What I would suggest is, given the fact that we still do have time in the remaining meetings to accommodate Mr. Amos, and given the uncertainty.... He is a member of Parliament, and he is around these parts more often than not, so it's easier to reaccommodate him. We would hear from the witness, do questioning and then, depending on how time is going, move on from there, and put Mr. Amos' testimony to another day.

[*Translation*]

I would like to hear what committee members think.

Let us start with Mr. Graham.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Mr. Amos plans to attend the meeting in any case. He has arranged to be replaced in his duties in order to be here.

I suggest that we do all the work we can until there are no further questions. If there is no vote in the House, the PayPal representative could appear for 45 to 60 minutes, depending on the number of questions. Then Mr. Amos could have the time to give his presentation at the end.

The Vice-Chair (Mr. Matthew Dubé): It is a possibility, but the problem—and this is what concerns me—is that Mr. Amos is sponsoring the motion. We may not have an opportunity to question him if it is nearly 5:30 p.m. or if the bells call us to vote.

The clerk informs me that this would have little effect on our schedule in the next weeks before the end of the session.

That is my personal, very sincere opinion. I am replacing Mr. McKay, but I do not want to impose my point of view. Even so, because of the number of days we have left, we may well not be able to move forward the study that Mr. Amos is asking for in a meaningful way.

I am still open to your suggestion, Mr. Graham.

What do you think, Mr. Paul-Hus?

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): I agree with you, Mr. Chair.

Mr. Johnson from PayPal has been waiting for an hour. Let us hear his presentation and take the time to ask our questions properly. Then we can adjourn.

Mr. Amos can appear at another time.

The Vice-Chair (Mr. Matthew Dubé): Does anyone object to proceeding in that way?

It seems unnecessary to do otherwise.

Mr. David de Burgh Graham: It depends when we will be able to come back.

A motion has been unanimously adopted by the House recommending that we undertake this study. I want to ensure that we come to grips with it as quickly as possible. This must not drag on for another month. We have already lost our time today.

That is why I suggest that Mr. Amos introduce his motion. That way, we can move on with the study.

The Vice-Chair (Mr. Matthew Dubé): Once again, the clerk has informed me that there is no problem with the schedule. I have checked the information. Mr. Graham, that may reassure you about our ability to hear from Mr. Amos at another time. As Mr. Paul-Hus said, we have already kept our witness waiting.

We have an hour and a quarter, but, even if this witness's testimony takes only 45 minutes and Mr. Amos then appears, we still may run out of time or be called to vote. So I prefer to avoid that uncertainty, especially considering the ease with which we can invite an MP to another meeting. With most witnesses, we can rarely do that.

So let us continue the meeting.

● (1620)

Mr. David de Burgh Graham: Okay.

Let us begin; let us not waste any more time.

[*English*]

The Vice-Chair (Mr. Matthew Dubé): Thank you, colleagues.

I will now move to our witness. I want to thank Mr. Johnson for his patience. The procedural wrangling that goes on in this place does have that impact sometimes. Joining us by video conference, we have Brian Johnson, who is Senior Director for Information Security at PayPal.

You have 10 minutes, Mr. Johnson, for your opening statement. We'll take questions from the members, and we thank you for taking the time this afternoon.

Mr. Brian Johnson (Senior Director, Information Security, PayPal, Inc.): Thank you very much. Good afternoon, Mr. Chairman and members of the committee.

Again, my name is Brian Johnson and I do serve as the Senior Director of Information Security at PayPal. I appreciate your giving us the opportunity to speak with you today and for making the time in your busy schedule.

I suspect you all know a bit about PayPal generally speaking, but allow me to add a bit of detail.

Founded in 1998, PayPal is a leading technology platform company that enables digital and mobile payments on behalf of more than 277 million consumers and merchants in more than 200 markets worldwide. We offer online and mobile merchant acquiring and money transfer services. PayPal is the most popular digital wallet in Canada.

We are based in San Jose, California, and our Canadian headquarters is in Toronto with offices in Vancouver. PayPal Canada was incorporated in 2006. We have more that 7.1 million customers including more than 250,000 small business customers in Canada.

Fuelled by a fundamental belief that having access to financial services creates opportunity, PayPal is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy. Our open digital payments platform gives PayPal's 277 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online or on a mobile device. Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money, and offers choice and flexibility when sending payments, paying or getting paid.

We believe now is the time to reimagine money and to democratize financial services so that managing and moving money is a right for all citizens, not just the affluent. We believe that every person has a right to participate fully in the global economy. We have an obligation to empower people to exercise this right and improve their financial health. As a fintech pioneer and an established leader, we believe in providing simple, affordable, secure and reliable financial services and digital payments that enable the hopes, dreams and ambitions of millions of people around the world. We have a fundamental commitment to put our customers at the centre of everything we do.

Securing our customers and their data is central to our mission. For financial companies, data security is the main pillar. Through strong partnerships, strategic investments and a tireless commitment to protecting consumers, PayPal has resolved to be an industry leader in cybersecurity capabilities and to help make the Internet safer.

We have in our favour more than 20 years of experience in processing electronic transactions safely. PayPal has one of the most sophisticated fraud prevention engines in the world, which gets smarter with every transaction that goes through our system. With our advanced fraud monitoring technology, we detect and prevent attacks before they happen.

Security is in our DNA, and it's at the epicentre of all that we do at PayPal. We are the number one trusted brand of e-commerce and mobile commerce around the world. People trust PayPal because they know that we don't share customers' financial information with merchants, retailers or online sellers. Our robust security standards ensure that every part of a transaction is safe and secure.

At PayPal we believe we have a responsibility to help protect our users against harm. Privacy has always been one of our main concerns. Our customers trust us with their data. We take that trust very seriously. We collect only the data that's necessary to fulfill services that a customer requests, to improve product experiences and deliver relevant PayPal advertisements and to prevent fraud. We never sell or rent customer information.

It's commonly held among global law enforcement agencies that cybercrime and online methods of fraud are now more common than crimes committed in the offline and physical world. As the committee is certainly aware, over the last five years, the RCMP alone has observed an almost 50% increase in cybercrime reports from Canadians. I applaud the committee for aggressive action and for its support of Canada's national security strategy, by including significant funding for investments in cybersecurity as part of your commitment to safety and security. Building an innovative and adaptive cyber-ecosystem is a crucial step to being able to quickly scale and combat emerging threats to critical infrastructure, government, business and individuals' digital information.

To conclude, I would like to emphasize PayPal's commitment to cybersecurity and our willingness to work together with the Canadian government and industry.

Thank you again for the invitation to discuss these very relevant topics and to represent PayPay's strong position in support of consumer data protection and privacy.

● (1625)

I'd be happy to answer any questions you may have.

The Vice-Chair (Mr. Matthew Dubé): Great. Thank you so much, Mr. Johnson.

We will proceed to our question period. We will begin with Ms. Sahota, please, for seven minutes.

Ms. Ruby Sahota (Brampton North, Lib.): Thank you, Mr. Johnson, for being here today.

Are there any differences in how you operate in Canada versus the U.S., or are you mainly based out of the U.S. and that's where all the information ends up when Canadians are using your service?

Mr. Brian Johnson: [*Inaudible—Editor*] by PayPal customers are stored within U.S. data centres and localized data housing, so localization of data of Canadian customers is also contained within the U.S.-hosted facilities.

Ms. Ruby Sahota: To clarify, there's no difference in how you operate when it comes to Canadian customers versus the American customers, right?

Mr. Brian Johnson: Other than localization for currency or for other preferences that are localized, the data and information is stored the same as that of U.S.-based customers.

Ms. Ruby Sahota: I'm very glad to hear that, because I would figure after operating for two decades—longer than other competitors in this realm have existed—you must have a lot of data stored up. It is good to hear that you don't sell the data that you have received. Thank you for providing us with that information.

However, I have seen that there have been several articles in just this recent month about PayPal. One is about paying hackers—I would assume they are white hat hackers—to try to protect the security of your system. Could I hear a little more about that, and how that's been working? Have you been doing that for a long period? Is this a recent trend, that you're paying hackers to hack your system? What advantages are you getting out of that?

Mr. Brian Johnson: That's an excellent question, Ms. Sahota.

Our program is called bug bounty, and it's an industry-wide accepted method of using contracted support, basically using the industry of white hat hackers through a managed program. They're vetted so they're not allowed to just go rogue or attack systems without request and without knowledge. They're considered professional security researchers across industry, and many of them are professionals in other areas and use freelance time or side jobs at times to provide what's called bug bounty ethical hacking. It helps us to expose any concerns or vulnerabilities in systems that are not caught with internal tools and to instead catch those through bug bounty programs, which again are commonly used by many companies for the security researcher community to collaborate with us on those vulnerabilities.

Ms. Ruby Sahota: Do you have contracts with these hackers?

Mr. Brian Johnson: We contract with a group called Hackerone that provides the vetting process with them, and then through responsible disclosures, those vulnerabilities are reported to us to fix them before they're disclosed publicly, so we can resolve any of those vulnerabilities that they find.

Ms. Ruby Sahota: If an issue was to occur where somebody was to breach the system or someone's privacy, where would the liability lie? Would it lie with PayPal?

Mr. Brian Johnson: If there's a system breach, that's an unauthorized activity and it would be treated as malicious and illegitimate access as with any mal-intended attacker. We don't have bug bounty researchers perform attacks or breaches, and as part of the program policy, they're not allowed to access customer data nor to make any manipulation or changes of information. They're allowed to disclose vulnerabilities that are detected in the system and report those to us through the responsible disclosure program.

Ms. Ruby Sahota: PayPal also uses an app for convenience for customers, correct?

● (1630)

Mr. Brian Johnson: An app for convenience? We do have a mobile app.

Ms. Ruby Sahota: A mobile app, that's right.

Mr. Brian Johnson: Correct, we do have mobile apps.

Ms. Ruby Sahota: I have seen articles also just recently this month of actual accounts of people being defrauded, with up to $9,000 or so being taken out of their bank account, and it has been done because the app can be hacked. As a result, the vulnerability of the app is allowing access into people's bank accounts directly.

We heard from credit card companies that the information is never shared directly. People's bank information does not directly go to the credit card company, but it seems in this case, the bank information is being directly shared with PayPal and then if there's a vulnerability there, the hacker can access all the information.

How are you protecting against that?

Mr. Brian Johnson: Media reports are not always accurate. To be technically accurate, the access of information within the PayPal account would only be through an authorized account holder or through their loss of credentials and device. If there's a loss of credentials by a consumer—let's say they have malware on their computer and their log-in credentials are stolen or lost through that—the access of their account through a malicious attempt would be caught by our fraud platform or risk systems to detect that. If it's not caught by some vulnerability, the only access into the PayPal account would be to PayPal balance, but not directly into the consumer's bank information. The bank information is stored in our system and not made visible, even after entered into the system by the consumer.

The only method they would have is of trying to extract data by using the PayPal system to process transactions. They might try to attempt fraud, but they wouldn't be able to get their bank account information through the platform.

Ms. Ruby Sahota: That's interesting. The article warns people to check their bank accounts regularly and look for PayPal transactions that may not have been authorized.

When this occurs, how does the person recover? Do they recover from their bank? Are they able to recover from PayPal?

Mr. Brian Johnson: We have buyer protection so if there are malicious or unintended transactions on a consumer account, we provide buyer liability and buyer protection for those fraudulent transactions and protect the consumer in that case.

I want to reiterate though that a malicious account access into a PayPal account is unlike a malicious access into any account. If online fraud occurs, we cover liability for the buyer, for the consumer, in that case. Our seller protection has other coverages to sell our merchants. The access to the PayPal account does not mean that the malicious actor necessarily has access to the bank account directly. They don't have access to credentials, nor to the bank account information, but only the linkage that we provide for the bank account as a funding instrument into the PayPal account.

Ms. Ruby Sahota: Okay.

I used PayPal many years ago, but I stopped using after a while when I continued to get fraudulent emails telling me about certain transactions that were made. I have a final comment; it can lead to being very confusing for the user and, therefore, I steered away from it because I found I was receiving too many fake emails from PayPal.

The Vice-Chair (Mr. Matthew Dubé): Unfortunately, we're going to have to leave it there.

[*Translation*]

I now give the floor to Mr. Paul-Hus for seven minutes.

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

Here is my first question.

Mr. Johnson, you mentioned that PayPal has existed since 1998. You have therefore been in existence since the beginnings of the Internet.

We know that cybersecurity issues have evolved in parallel with the Internet. Is PayPal able to follow that evolution and counter those threats?

[*English*]

Mr. Brian Johnson: Many of our staff in our information security organization are members of industry alliances that are helping to make the Internet more secure. We are absolutely in the research and development stages of many investments. Email phishing and anti-phishing working groups are other areas as well, as Ms. Sahota mentioned. The investments we make in email security, Internet security and browser security are at the forefront of our investments.

● (1635)

[*Translation*]

Mr. Pierre Paul-Hus: You also mentioned that people trust PayPal.

What measures have you undertaken to ensure that those who do business with PayPal do so with complete trust?

[*English*]

Mr. Brian Johnson: As I mentioned, our buyer protection programs provide liability coverage for any fraudulent activities that might happen on a consumer account. We also invest heavily into cybersecurity initiatives and our fraud-risk platforms. We have industry-leading metrics on how low our fraud numbers are in the sense that we protect and prevent a significant amount of fraud, and protect merchants and consumers on our platform at an excellent rate that we're very proud of.

[*Translation*]

Mr. Pierre Paul-Hus: Excellent.

Among the witnesses who have appeared before our committee for this study, we have had representatives from a number of banks, including the Toronto-Dominion Bank. One of its representatives informed us that cyber attacks against the bank come from a number of different countries.

Can you name the countries attacking PayPal's system?

[*English*]

Mr. Brian Johnson: Interestingly, foreign countries—you mention nation-state, and it's not information I'm at liberty to share, but related to private attackers or individuals who are online fraudsters who would attempt to attack websites happens on a regular basis. They're not centralized to any particular geographic region. There is, of course, a high distribution of cyber-attacks where their origin or their attribution to the country of origin is often difficult to trace, because a lot of countries participating in their infrastructure are allowing it to be hacked. As an example, attackers may originate from one country and use Internet services from another country to direct their attacks. Criminals use a multi-layered economy, and multiple parties are usually involved from different regions of each attack.

[*Translation*]

Mr. Pierre Paul-Hus: I understand the difference between an individual's country of origin and the country from which an attack comes, but my question was more about the countries than the individuals. Has PayPal been subject to attacks from states?

[*English*]

Mr. Brian Johnson: Not in particular. We have no singular concentration of countries that attack us as a company uniquely.

[*Translation*]

Mr. Pierre Paul-Hus: Okay, perfect.

Your company is based in the United States and deals with many different countries, all of which have different regulations. Given that we are studying this from a Canadian perspective, do Canadian laws and regulations have an effect on PayPal's activities? For example, are our privacy laws too restrictive or not restrictive enough?

[*English*]

Mr. Brian Johnson: It's an excellent question. The data protection and data privacy implications that Canada is proposing and has outlined as a framework are an excellent support for industry and businesses globally.

To answer the first part of your question about operating globally, we do have staff in many of our regions that have increased regulations. We gave a local presence in many countries, including Europe, with support for GDPR, and in regions in Singapore where we have support for our business in the APAC region. We do have localized staff and support for each of those regions, as well as in other areas in the world that support local regulations. We have a global workforce that encourages participation with local legislators and regulators. We work closely with examiners and regulators when there are data protection and data privacy laws to ensure that we not only support and accommodate those, but help to align with regulations that are evolving and help inform practical applications to those in a context that's suitable for a global economy.

[*Translation*]

Mr. Pierre Paul-Hus: In your opinion, are there aspects that Canada should improve? You have said that our country has strong laws, but do you still have recommendations for us on the legislative level?

● (1640)

[*English*]

Mr. Brian Johnson: By the way, on the announcement of the new digital charter, PayPal applauds Minister Bains and the Government of Canada for taking leadership on that important topic of data protection. We believe that this responsibility does help us to protect users against harm and support privacy laws. It's a great first step. It derives some principles. I believe the 10th principle, or the last one on that was to provide accountability and enforcement. More detail around that would be helpful.

Certainly, as Canada has not been the first mover of data privacy law, I think that's actually worked to your advantage because you've been able to learn from other regions and regulators about the right balance of privacy law. But in being specific with companies with respect to the digital privacy and regulations that you're encouraging, there will be a tough balance between the framework that you've provided and those guiding principles that help direct good behaviour and strong accountability. As well, the work with industry and private partnerships will help to build strong legislation that you can support in years to come.

[*Translation*]

The Vice-Chair (Mr. Matthew Dubé): Thank you very much.

We will now give the floor to Mr. Picard for seven minutes.

Mr. Michel Picard (Montarville, Lib.): Mr. Chair, usually, you would also have the right to speak for seven minutes.

Under the circumstances, I propose allowing the Chair seven minutes so that he can ask questions on behalf of his party.

The Vice-Chair (Mr. Matthew Dubé): You are very generous, thank you.

[*English*]

Mr. Michel Picard: I won't do that again.

Sir, I would like to look at your operation from a money-laundering standpoint. When I buy credit or I put money in my account, my first naive question is where does my money go?

Mr. Brian Johnson: Where does your money go in a PayPal balance stream?

Mr. Michel Picard: Yes.

Mr. Brian Johnson: PayPal balances are backed by a number of U.S. banks, so we support depositing and safe investment and deposit of the account money. The first item was if you use credit. Was that a supporting comment, or what was the line there, before I answer?

Mr. Michel Picard: When I buy a number of credit...and I put some money in my account for further purchases, my money then ends up in a bank supporting your transaction. Let's say I have $100 of whatever unit, or it might be just dollars, to buy stuff. Do you trace the origin of this transaction and where it comes from, whether credit card, bank account or stuff like that?

Mr. Brian Johnson: Yes, I'm sorry. I understand your question now, Mr. Picard.

Yes. The origin of the money.... From an anti-money laundering, AML, perspective, we have an anti-money laundering department and a strong division and investment in detecting money-laundering activities. We treat those activities very seriously by tracing the money trail from the point of origin, funding source and the original deposit method, and we support law enforcement efforts in fighting any money-laundering operations or fraud schemes that are detected or reported on the platform.

Mr. Michel Picard: You are supporting efforts during the investigation, but when you get the money from any credit card, at your level, I guess you accept the transaction as long as there is enough money at the point of origin. That means that if I have, for example, a prepaid credit card, and I want to put money in my balance, I put in mu credit card, you verify the balance, the money is there, you take it, and there's no more investigation, regardless of the origin. Whether this origin is criminal or not, you cannot verify that.

Mr. Brian Johnson: We actually do validation of the data source or the money source at its origin, and in certain circumstances, prepaid has limits supplied on how much money we will allow to be deposited and what money can be withdrawn within a period of time or spent within certain websites. Our risk and fraud platforms do have very granular rules that detect certain financial instruments that are used based on the risk level. If there is an AML or a money-laundering method that we've written into our fraud patterns for that use case, like prepaid, as an example, we place limits and certain criteria to restrict losses and to minimize risk in that case.

● (1645)

Mr. Michel Picard: Do you have pattern analysis in terms of types of transactions?

Mr. Brian Johnson: We do. We perform behavioural analysis, and we have some artificial intelligence methods running in our risk platforms that are learning and baselining behaviours and payment patterns across the platform.

Mr. Michel Picard: Usually when money is in my balance, I cannot withdraw money as is. I have to buy something. Is that the case, or do I have exceptions where I can withdraw some money from my balance?

Mr. Brian Johnson: We do provide methods of withdrawing money in certain regions of the world, depending on where the money was sourced, of course. It can be withdrawn through different methods. We have a partnership, as an example, with Walmart that allows for cash withdrawals. With Walgreens and with local retailers, we've opened partnerships that allow for deposit and withdrawal of cash in local currency. Through our integration with the Zoom platform, we also allow for global remittance or transfer across borders of different transactions and withdrawal of money through different methods at retailers as well. The money can also be deposited or withdrawn in cash by certain methods.

Mr. Michel Picard: What is the maximum amount of money I can put in my balance in one transaction?

Mr. Brian Johnson: I believe it depends on the risk rules. That's not my area of expertise, so I don't know the specifics, but there are limits depending on the age of the account, whether your account has been verified with identification and whether we've verified the account holder's history. There are other methods of raising that limit based on knowledge and know-your-customer indicators on trusting the account holder.

Mr. Michel Picard: Do you have the obligation to declare to FINTRAC in Canada if there are patterns of transactions or deposits of more than $10,000?

Mr. Brian Johnson: I'm not certain about that. I'm not in the fraud or AML department, but I know that we do report through FinCEN and other networks in the U.S. that I'm familiar with with respect to certain criteria. I'm not familiar with our reporting through the fraud pattern notification with Canada, though. We can certainly find out.

Mr. Michel Picard: If I put money in my own account so I can, myself, withdraw my own money without your knowing whether I'm the same person doing the two transactions.... Let's say I take a prepaid card, or my money is in an account in a bank that is the same, under suspicion, because we do have some banks that are under suspicion.

Mr. Brian Johnson: Sure.

Mr. Michel Picard: I put money in my PayPal account. Two or three days after that, I withdraw my money. The only information you need to know to do this transaction is whether the account has the right log-in and password to get in, and the same thing to get the money out. There's no possibility to verify whether it's the same person. My colleague and I may work on the same account.

Mr. Brian Johnson: We do verify device telemetry. We look for information about the device, the computer you're using, based on geolocation, on some other fraud detection patterns, to try to verify the authenticity of the user on the account. The account holder, of course, has to have the credentials to perform that payment or that transaction.

Mr. Michel Picard: Another area—I don't have much time—is the nature of the attacks where you've been targeted.

What kind of evolution have you seen throughout the years, the level of sophistication of those attacks? What can you say about that?

Mr. Brian Johnson: Generally speaking, the cyber-attack footprint has become much more complex and advanced. Cyber-criminals have become much more of an economy unto themselves, and have layered their tools, their data, their methods of attack in a very sophisticated way, and in a very coordinated way in many cases.

Criminals are creating tools, and both executing and renting access to those tools. Distributed denial-of-service attacks, or DDoS attacks, have become much more significant and advanced over the years. The cyber-landscape in threats and emerging trends in that area have definitely become more complex, and have increased in scale dramatically in recent years.

Mr. Michel Picard: Thank you.

The Vice-Chair (Mr. Matthew Dubé): Colleagues, as you can see, we have bells. We require unanimous consent to continue. If we choose to do so, we must also decide for how much longer we will continue. I'm looking for guidance, based on the number of questions you may or may not have.

Mr. Graham.

Mr. David de Burgh Graham: I say we go until the bells flash three times, which should give us five minutes to get upstairs.

The Vice-Chair (Mr. Matthew Dubé): You're proposing that we go for 20 minutes?

Mr. David de Burgh Graham: Twenty-two more minutes, yes.

An hon. member: Is that enough time?

Mr. David de Burgh Graham: It's five minutes to go up two floors in this building.

The Vice-Chair (Mr. Matthew Dubé): Can we agree on two final five-minute rounds for each of the parties at the table right now? Is that okay?

Some hon. members: Agreed.

An hon. member: Do you want [*Inaudible—Editor*], Mr. Chair ?

The Chair: I'm good on my end, but I appreciate the generosity with the speaking time from your side.

Mr. Eglinski, please, for five minutes.

● (1650)

Mr. Jim Eglinski (Yellowhead, CPC): I'd like to thank the witness for being here.

Brian, I want to follow through with what Mr. Picard was stating.

You stated earlier in your evidence that the money put into the PayPal accounts goes into the United States. Is that true for all countries where you do transactions?

Mr. Brian Johnson: I'm not certain on that, Mr. Eglinski.

I'd have to verify with our product team on where the money is deposited in back-end sources based on locale.

Mr. Jim Eglinski: Let's deal with the Canadian customers.

Do all the funds from which we do transactions with you go into the United States, or is some of it done here in Canada?

Mr. Brian Johnson: I'm sorry. I'm not sure which products have storage of data and balances in which accounts, so I can't answer that with clarity.

Mr. Jim Eglinski: All right.

Is there a regulatory body in the United States that requires you to report breaches in your program? As you mentioned to Mr. Picard earlier, you have a program that will kick out if a transaction is made and a second transaction is withdrawn from a different locale.

Is that requirement for you? Do you report those to certain security agencies within the United States or Canada?

Mr. Brian Johnson: We have a number of obligations to notify and notification obligations based on regulators across the globe. Again, those are regionally managed at the state level within the U. S., and at the regional level within each of the regulators.

We're governed by the CSSF in Europe, which is overseeing our European banking licence, and the MAS, which is the Monetary Authority of Singapore. We're governed in a number of other jurisdictions where we operate money remitter and payment service provider licences that we do in the United States and Canada.

Those obligations to notify vary based on the condition, but we do notify regulators of occurrences on whether they cross the threshold of notification for any data breach situation, or for any money-laundering operation or fraud scheme that we may detect on the platform. Those are notified through regulators as required.

Mr. Jim Eglinski: Are you a member of the Canadian Cyber Threat Exchange?

Mr. Brian Johnson: No, sir, we're not. We've discussed with the group, and our threat intelligence team has met with them before, but we're not currently members of the group.

Mr. Jim Eglinski: Is there a reason for that?

Mr. Brian Johnson: I believe there were other channels that superceded that—threat exchange platforms that are not specifically regional. The CCTX actually subscribes to some of the threat feeds that we're already members of. There are a number of threat exchanges that I believe they already exchange data through. We're not opposed to it, there just wasn't a need, as we've discussed with them, for any unique data exchange.

Mr. Jim Eglinski: Okay, thank you.

I've been a member of PayPal, I think since about 2000, and have used it quite often over the years.

Mr. Brian Johnson: Thank you for your business.

Mr. Jim Eglinski: How much of my personal information, or other users', goes through your service? Where is that information stored? Is it all stored in the United States, or is it stored in individual countries?

Mr. Brian Johnson: It's all stored in the United States. Personal information is all encrypted. We have extremely high-level encryption technologies at all levels of our infrastructure and technology stack. Personally identifiable information is not shared. Again, we don't sell or rent that data out to anyone, for marketing or any other purpose. It is housed and stays on PayPal's systems in the United States, in our data centres.

Mr. Jim Eglinski: Have you been hacked?

Mr. Brian Johnson: Have we been hacked? The direct answer is that we have not been breached. If you're asking if we've been breached in the sense of a customer-notifiable data breach event from PayPal, no. Properties, as you may be aware, of other adjacent companies that we've acquired over the years have reported cyber-incidents. We've had some vulnerabilities, and what would be classified as “hacks” noted in different products as an interface, but none of those have led to a massive breach, or a data loss at the extreme level that would require any notification.

Mr. Jim Eglinski: You mentioned that all the data is stored in the United States. Is it stored in only one facility, or do you have a backup-type system?

● (1655)

Mr. Brian Johnson: We have multiple backups, yes. We're geographically distributed across high-availability data centre zones, so that we maintain resilience and disaster recovery capabilities across the platform.

Mr. Jim Eglinski: Okay. Thank you.

[*Translation*]

The Vice-Chair (Mr. Matthew Dubé): Thank you, Mr. Eglinski.

We will now give the floor to Mr. Graham for the last five minutes.

[*English*]

Mr. David de Burgh Graham: I have a more lighthearted question to start with.

Do you know that at the bottom of the screen, it says, “SCF Superman”?

Mr. Brian Johnson: Yes, it does. That's my conference room.

Voices: Oh, oh!

Mr. David de Burgh Graham: Okay. I'm just wondering, because that's televised, so everyone is going to see that.

Mr. Brian Johnson: Yes. That's a joke, so you're just fine.

Mr. David de Burgh Graham: You mentioned that you don't trade data. Is there no interaction of any data, besides transaction data, between PayPal and any other company, for any reason? Would that be correct?

Mr. Brian Johnson: We don't sell or rent data. There are certain fraud detection and other methods that we use. There are certainly integrations with merchants where we require certain data types. We don't sell or rent our customer data. The customer data footprint is not exchanged with third parties for marketing purposes, unless it's opted in on the PayPal platform by our customers.

Mr. David de Burgh Graham: What data, besides transaction history data, does PayPal collect from its own customers, for some marketing purposes?

Mr. Brian Johnson: I'm sorry, Mr. Graham, I'm not in the marketing department, so I'm not sure which data elements the marketing department uses. Again, we don't rent or sell that data outside of the platform. I'm not sure what we use onside of the platform, and into our platform, from a marketing perspective. Do you mean if they source other data, in other words, or data that's collected from PayPal customers?

Mr. David de Burgh Graham: I'm just trying to get to the bottom of it. Mr. Picard and I just came out of three days of the grand committee on privacy, and we've discussed the avatars companies create, and this type of thing, so it's obviously top of mind for us and I'm trying to understand the level of information PayPal has on its users. Is it just: This person has sent this much money, and that's all we know about him, or is there a great deal more information retained by PayPal about their users?

Mr. Brian Johnson: Certainly from a financial perspective, and in regard to some of the prior questions around any money-laundering detection and fraud prevention, we need to collect more data around transaction details, usage of the platform and device information, to comply with local law enforcement and regulators that require us to maintain knowledge of customers.

From a know-your-customer, KYC, perspective, the transaction history and the usage of certain customer computers and devices are bits of information we use to detect fraud. Those are, again, not used for marketing purposes. We wouldn't market you because you have connected a certain device type to us, if, for example, we use that for fraud prevention. Again, to my knowledge, that's not information we would have in our marketing team's purview, to expand on or share outside of that function.

Mr. David de Burgh Graham: A couple of years ago, there was a lot of ink spilled over a class action lawsuit against PayPal for accepting donations to charities that weren't members of PayPal, and it was eventually referred to binding arbitration. By any chance, do you know the status of that suit?

Mr. Brian Johnson: I don't. I recall reading about it, but I don't recall the status of that suit.

Mr. David de Burgh Graham: Then it wouldn't be in your purview to discuss why PayPal would accept donations for clients they don't have.

Mr. Brian Johnson: I'm not in that space; I'm in the cybersecurity space.

As I understood, though, it was one of those situations where, as we accept for charities, whether we validate that the charity is a valid one was a concern in that case. I don't recall if it was outside that scope, because it wasn't in my purview.

Mr. David de Burgh Graham: In the time I have left, can you give us a bit of a taste of the evolution of PayPal cybersecurity?

You've been around since 1998, and an awful lot has changed in that time. Do you have some key moments that you'd like to tell us about?

Mr. Brian Johnson: Certainly.

PayPal was part of eBay until just five years ago, and at that point, eBay had encountered some cyber-events. We were part of a program that learned from those. We've emerged into the leading digital payments platform that has evolved into a global leader in this space.

We've certainly invested a lot in knowing the industry partners and working with government and working with public and law enforcement agencies to make sure that we understand the climate of each of the regions that we do business in. We've invested quite a bit in our fraud platforms to understand more about what types of criminals are trying to defraud customers. Of course, we've remained true to protecting customers data and standing behind them with our buyer protection program and safe practices in protecting consumers in all those situations.

Mr. David de Burgh Graham: Thank you for having come, because I know a lot of other companies in this sector haven't come to visit us. I really appreciate people taking the time to come and discuss these issues with us.

● (1700)

Mr. Brian Johnson: Thanks for inviting us.

The Vice-Chair (Mr. Matthew Dubé): Thank you, and I will echo those sentiments.

Mr. Johnson, thank you very much, not only for your time but also for your patience, as we were a bit delayed in getting started.

[*Translation*]

Thank you very much, colleagues.

Given the time and the fact that we have to go to vote, it serves no purpose for us to come back later. So I thank you for indulging me as Mr. McKay's temporary replacement, and add that our meeting is adjourned.

The meeting is adjourned.