

From: s. 47F
Date: 29 September 2018 at 2:35:25 am AEST
To: s. 47F

Subject: Important Update

Dear Ms Falk,

We wanted to alert you about an attack on our systems by an external actor that we are continuing to investigate. Please see the linked Newsroom Post for specific information, which will be issued shortly: <https://newsroom.fb.com/>

We are happy to schedule a call at your earliest convenience and answer any questions you may have.

Regards,

s. 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

From: s. 47F
To: [Amie Grierson](#)
Cc: s. 47F; [Melanie Drayton](#)
Subject: RE: Important Update [SEC=UNCLASSIFIED]
Date: Saturday, 29 September 2018 7:31:27 PM
Attachments: [image002.png](#)
[Megaphone.png](#)

Hi Amie,

Many thanks for speaking with me earlier today. As noted in the newsroom post (<https://newsroom.fb.com/news/2018/09/security-update/>), people with password issues can visit our Help Center. If anyone wants to contact us for any other information relating to the recent notification they can also do this via the [Help Center](#) (the contact form is available at <https://www.facebook.com/help/contact/861937627253138>) and which is available even if the person is not a user of, or logged in to, Facebook. There is also a physical address available to all users:

Facebook, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Logged in users can also contact us through the Report a Problem tool (available if a user clicks on the question mark at the top right hand corner of a user's profile). Our privacy operations team are responding to the user questions that come through these (and other channels).

Please see attached images of the message that Facebook is using to notify affected users. As you would see, there is a "Learn More" button. Clicking on that button will lead to this [page](#). The notifications are rolling out globally now and will be live to all users by early next week. Please note, you may not see the notification the first time you log back in. We will provide further updates as the investigation develops.

For your convenience, below is a screenshot of the page. Please feel free to reach out to either myself [s. 47F](#) for more information.

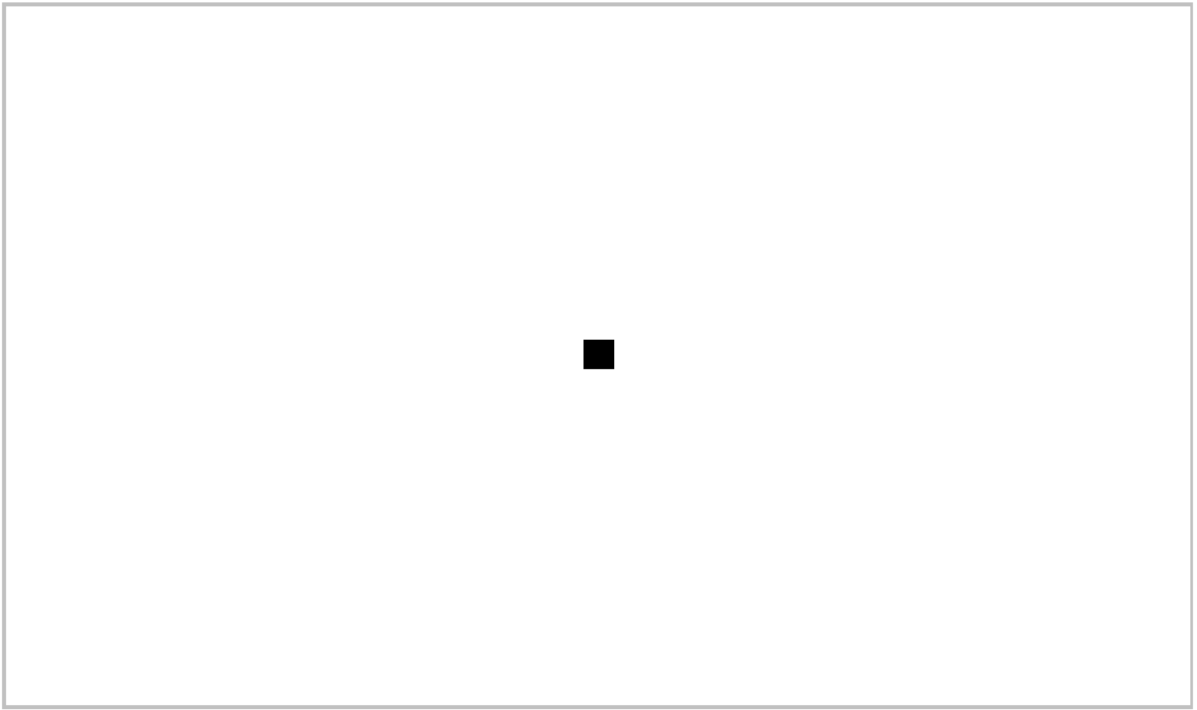
Kind regards,

[s.](#)

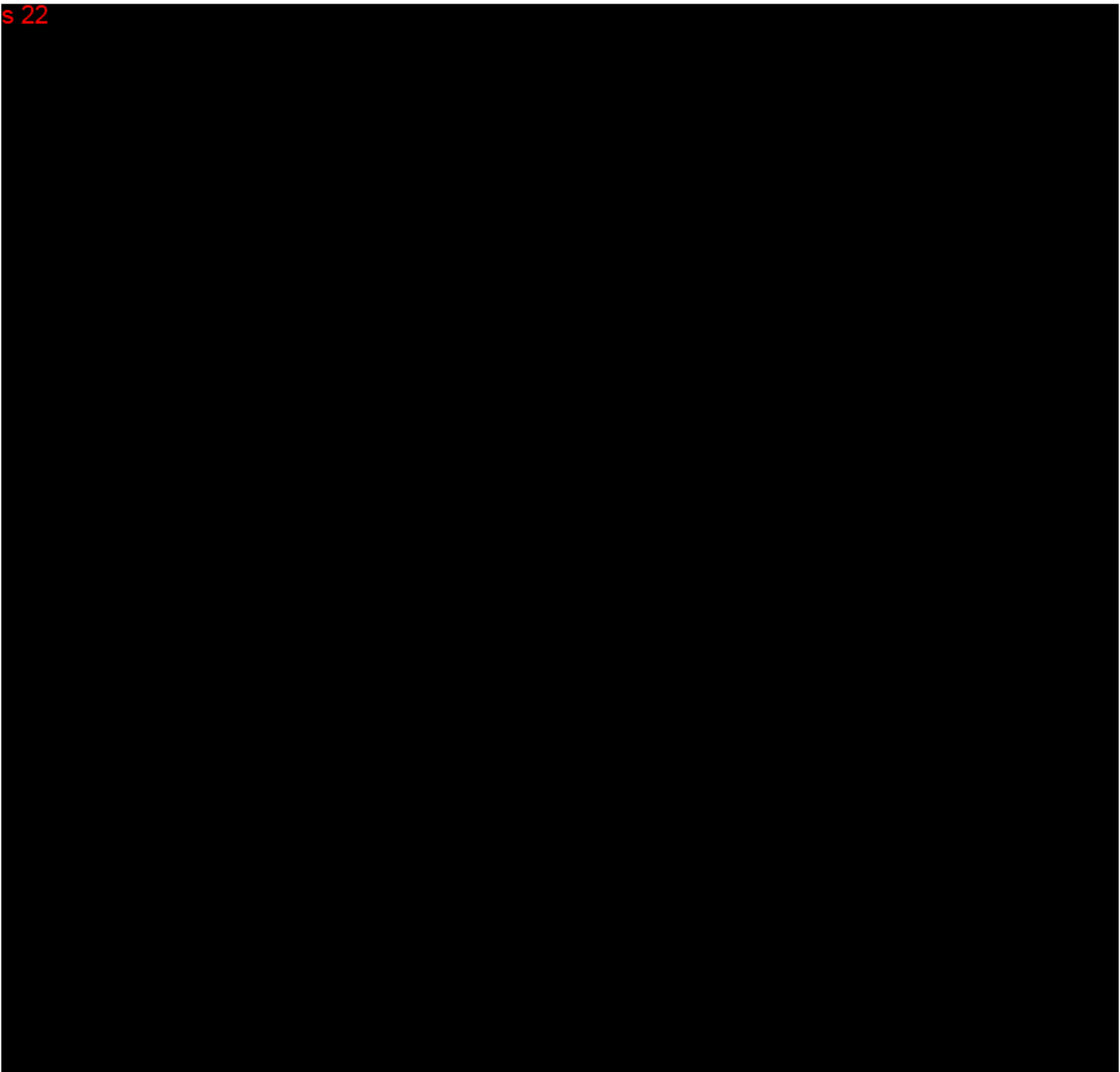
-

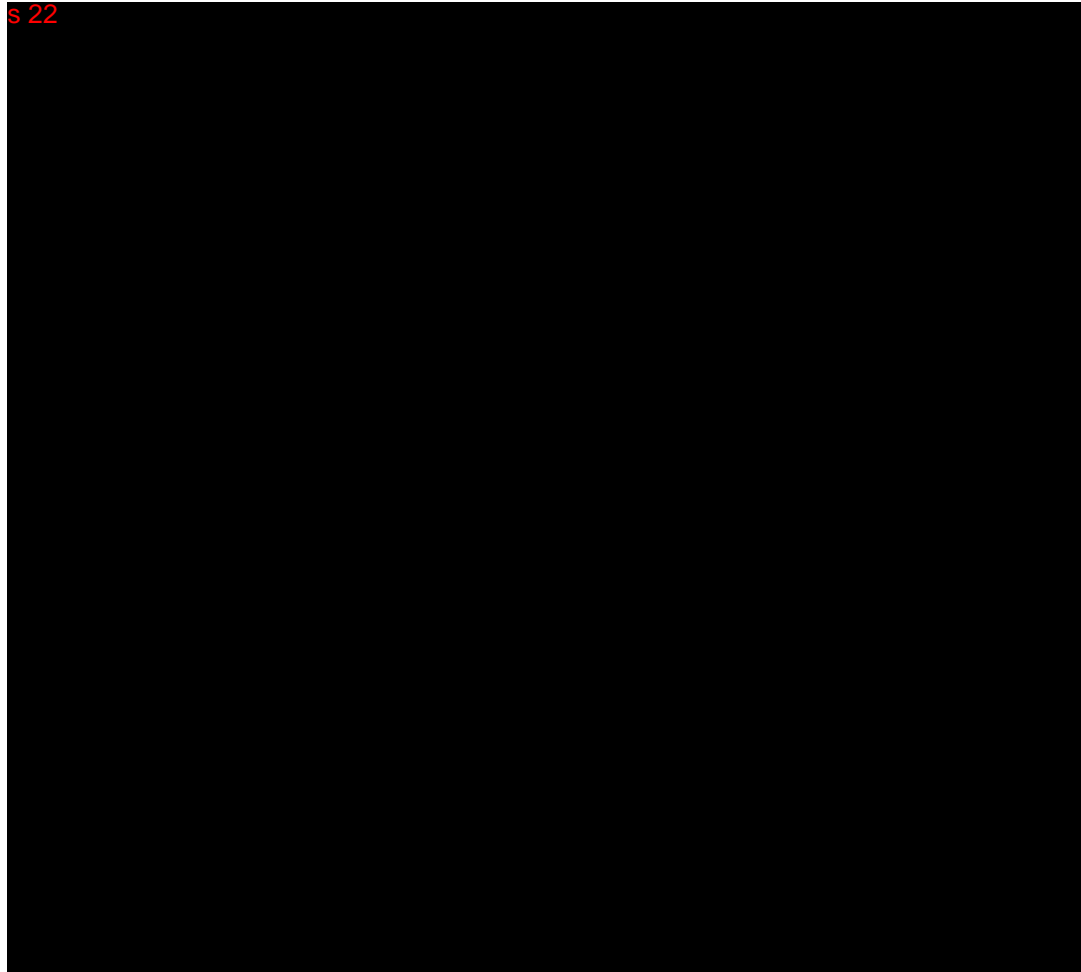
[s. 47F](#) | [facebook](#) | Legal | [47F](#)

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.



s 22





From: s. 47F
Date: 29 September 2018 at 2:35:25 am AEST
To: "angelene.falk@oaic.gov.au" <angelene.falk@oaic.gov.au>
Cc: s. 47F
[Redacted]
Subject: Important Update

Dear Ms Falk,

We wanted to alert you about an attack on our systems by an external actor that we are continuing to investigate. Please see the linked Newsroom Post for specific information, which will be issued shortly: <https://newsroom.fb.com/>

We are happy to schedule a call at your earliest convenience and answer any questions you may have.

Regards,

s. 47F | [facebook](#) | Legal, Privacy | 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.



From: S. 47F
To: [Amie Grierson](#)
Cc: S. 47F, [Melanie Drayton](#)
Subject: RE: Important Update [SEC=UNCLASSIFIED]
Date: Monday, 1 October 2018 7:13:27 AM
Attachments: [image003.png](#)

Dear Amie,

Please see our responses to your questions below. If you have any further questions please do not hesitate to contact S. 47F or myself.

1. Were any Australian Facebook accounts involved in the incident?

Our investigation is still in its early days and we're working hard to better understand these details. We don't know the location of all affected people. We also do not know if this was targeted to people from one particular country. We have so far found almost 50 million accounts that were affected. The security tokens for these accounts have already been invalidated to secure them. We've also taken the precautionary step of invalidating access tokens for another 40 million accounts that have been subject to a "View As" lookup. As a result, over 90 million people will now have to log back in to Facebook, or any of their apps that use Facebook Login. As we find more affected accounts, we will invalidate their access tokens — as well as the tokens of any more accounts we identify that have been subject to a "View As" lookup since July 2017.

2. If so, please advise how many Australians may have been impacted? *We will update you as soon as we know more details as to location of those affected.*

3. Whether at this stage you consider the incident to be an eligible data breach under the notifiable data breaches scheme? *At this stage we do not consider the incident to be an eligible data breach under the Australian notifiable data breaches scheme however we will continue to keep you and users informed about the incident and any developments.*

4. When did Facebook first become aware of the incident? *We became aware of the issue late on Tuesday 25th September 2018 (PST) (26th September 2018 (Syd))*

4. Any steps Facebook is taking to assess whether the matter is an eligible data breach for the purposes of the notifiable data breaches scheme, noting that eligible data breaches require notification to individuals and the OAIC under the scheme within statutory timeframes. *Our investigation is ongoing and we are continually assessing whether the incident is an eligible data breach under the notifiable data breaches scheme. We will continue to update both the OAIC and users with any developments.*

5. Whether there is specific information we might provide to individuals who may contact the OAIC with concerns about the incident, including how they can find out if they were impacted, what steps they should be taking to protect their privacy, and, if they wish to complain to Facebook about the incident, how they may do so. *Please alert them to the newsroom post <https://newsroom.fb.com/news/2018/09/security-update/> If they wish to contact Facebook directly they can do so through the channels as outlined in my email below.*

Kind regards

S. 47F

From: [REDACTED]
Sent: 4 Saturday, September 29, 2018 2:31 AM
To: 'Amie Grierson' <amie.grierson@oaic.gov.au>
Cc: s 47F [REDACTED]
[REDACTED] Melanie Drayton <melanie.drayton@oaic.gov.au>
Subject: RE: Important Update [SEC=UNCLASSIFIED]

Hi Amie,

Many thanks for speaking with me earlier today. As noted in the newsroom post (<https://newsroom.fb.com/news/2018/09/security-update/>), people with password issues can visit our [Help Center](#). If anyone wants to contact us for any other information relating to the recent notification they can also do this via the [Help Center](#) (the contact form is available at <https://www.facebook.com/help/contact/861937627253138>) and which is available even if the person is not a user of, or logged in to, Facebook. There is also a physical address available to all users:

Facebook, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Logged in users can also contact us through the Report a Problem tool (available if a user clicks on the question mark at the top right hand corner of a user's profile). Our privacy operations team are responding to the user questions that come through these (and other channels).

Please see attached images of the message that Facebook is using to notify affected users. As you would see, there is a "Learn More" button. Clicking on that button will lead to this [page](#). The notifications are rolling out globally now and will be live to all users by early next week. Please note, you may not see the notification the first time you log back in. We will provide further updates as the investigation develops.

For your convenience, below is a screenshot of the page. Please feel free to reach out to either myself s 47F [REDACTED] for more information.

Kind regards,

s [REDACTED]

-
s.47F [REDACTED] | [facebook](#) | Legal | 47F [REDACTED]

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

cid:image002.png@01D457FA.0AAB8380



s 22

s 22

s 22

s 22

From: §
Date: 29 September 2018 at 2:35:25 am AEST
To: "angelene.falk@oaic.gov.au" <angelene.falk@oaic.gov.au>
Cc: § 47F
Subject: Important Update

Dear Ms Falk,

We wanted to alert you about an attack on our systems by an external actor that we are continuing to investigate. Please see the linked Newsroom Post for specific information, which will be issued shortly: <https://newsroom.fb.com/>

We are happy to schedule a call at your earliest convenience and answer any questions you may have.

Regards,

§ 47F | [facebook](#) | Legal, Privacy | § 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

WARNING: The information contained in this email may be confidential.
If you are not the intended recipient, any use or copying of any part
of this information is unauthorised. If you have received this email in
error, we apologise for any inconvenience and request that you notify
the sender immediately and delete all copies of this email, together
with any attachments.

From: s 47F
To: [Amie Grierson](#)
Cc: s 47F [Melanie Drayton](#)
Subject: RE: Important Update [SEC=UNCLASSIFIED]
Date: Monday, 1 October 2018 2:29:17 PM
Attachments: [image003.png](#)

Hi Amie,

To add to the below, both users and non users can also email Facebook directly via the alias datarequests@support.facebook.com. If you do share this with people (please feel free to do so) could you please ask them to reference the issue in the subject line i.e. please reference "Australia" and "Access Token" in the subject line, that will help our teams to track and prioritize reports. (People do not have to do this to receive a response but it would assist us in managing these requests).

Please do not hesitate to contact us with any questions.

Regards

s

From: s 47F
Sent: Sunday, September 30, 2018 2:13 PM
To: 'Amie Grierson' <amie.grierson@oaic.gov.au>
Cc: s 47F [Melanie Drayton](#) <melanie.drayton@oaic.gov.au>
Subject: RE: Important Update [SEC=UNCLASSIFIED]

Dear Amie,

Please see our responses to your questions below. If you have any further questions please do not hesitate to contact s 47F

1. Were any Australian Facebook accounts involved in the incident?
Our investigation is still in its early days and we're working hard to better understand these details. We don't know the location of all affected people. We also do not know if this was targeted to people from one particular country. We have so far found almost 50 million accounts that were affected. The security tokens for these accounts have already been invalidated to secure them. We've also taken the precautionary step of invalidating access tokens for another 40 million accounts that have been subject to a "View As" lookup. As a result, over 90 million people will now have to log back in to Facebook, or any of their apps that use Facebook Login. As we find more affected accounts, we will invalidate their access tokens — as well as the tokens of any more accounts we identify that have been subject to a "View As" lookup since July 2017.
2. If so, please advise how many Australians may have been impacted? *We will update you as soon as we know more details as to location of those affected.*
3. Whether at this stage you consider the incident to be an eligible data breach under the notifiable data breaches scheme? *At this stage we do not consider the incident to be an eligible data breach under the Australian notifiable data breaches scheme however we will continue to keep you and users informed about the incident and any developments.*
4. When did Facebook first become aware of the incident? *We became aware of the issue late on Tuesday*

25th September 2018 (PST) (26th September 2018 (Syd))

4. Any steps Facebook is taking to assess whether the matter is an eligible data breach for the purposes of the notifiable data breaches scheme, noting that eligible data breaches require notification to individuals and the OAIC under the scheme within statutory timeframes. *Our investigation is ongoing and we are continually assessing whether the incident is an eligible data breach under the notifiable data breaches scheme. We will continue to update both the OAIC and users with any developments.*

5. Whether there is specific information we might provide to individuals who may contact the OAIC with concerns about the incident, including how they can find out if they were impacted, what steps they should be taking to protect their privacy, and, if they wish to complain to Facebook about the incident, how they may do so. *Please alert them to the newsroom post <https://newsroom.fb.com/news/2018/09/security-update/> If they wish to contact Facebook directly they can do so through the channels as outlined in my email below.*

Kind regards

s [REDACTED]

From: s 47F [REDACTED]

Sent: Saturday, September 29, 2018 2:31 AM

To: 'Amie Grierson' <amie.grierson@oaic.gov.au>

Cc: s 47F [REDACTED]

[REDACTED] Melanie Drayton <melanie.drayton@oaic.gov.au>

Subject: RE: Important Update [SEC=UNCLASSIFIED]

Hi Amie,

Many thanks for speaking with me earlier today. As noted in the newsroom post (<https://newsroom.fb.com/news/2018/09/security-update/>), people with password issues can visit our [Help Center](#). If anyone wants to contact us for any other information relating to the recent notification they can also do this via the [Help Center](#) (the contact form is available at <https://www.facebook.com/help/contact/861937627253138>) and which is available even if the person is not a user of, or logged in to, Facebook. There is also a physical address available to all users:

Facebook, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Logged in users can also contact us through the Report a Problem tool (available if a user clicks on the question mark at the top right hand corner of a user's profile). Our privacy operations team are responding to the user questions that come through these (and other channels).

Please see attached images of the message that Facebook is using to notify affected users. As you would see, there is a "Learn More" button. Clicking on that button will lead to this [page](#). The notifications are rolling out globally now and will be live to all users by early next week. Please note, you may not see the notification the first time you log back in. We will provide further updates as the investigation develops.

For your convenience, below is a screenshot of the page. Please feel free to reach out to either myself s 47F [REDACTED] for more information.

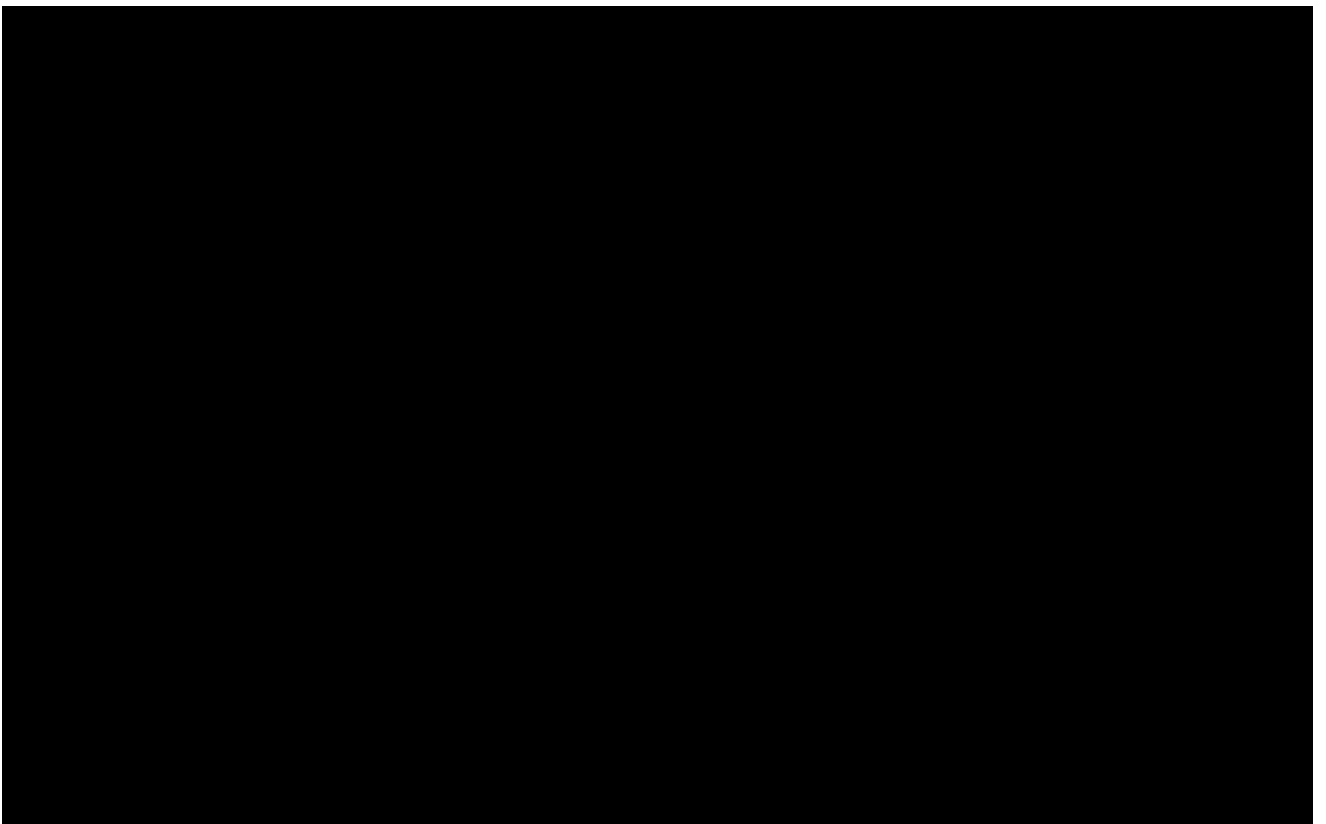
Kind regards,

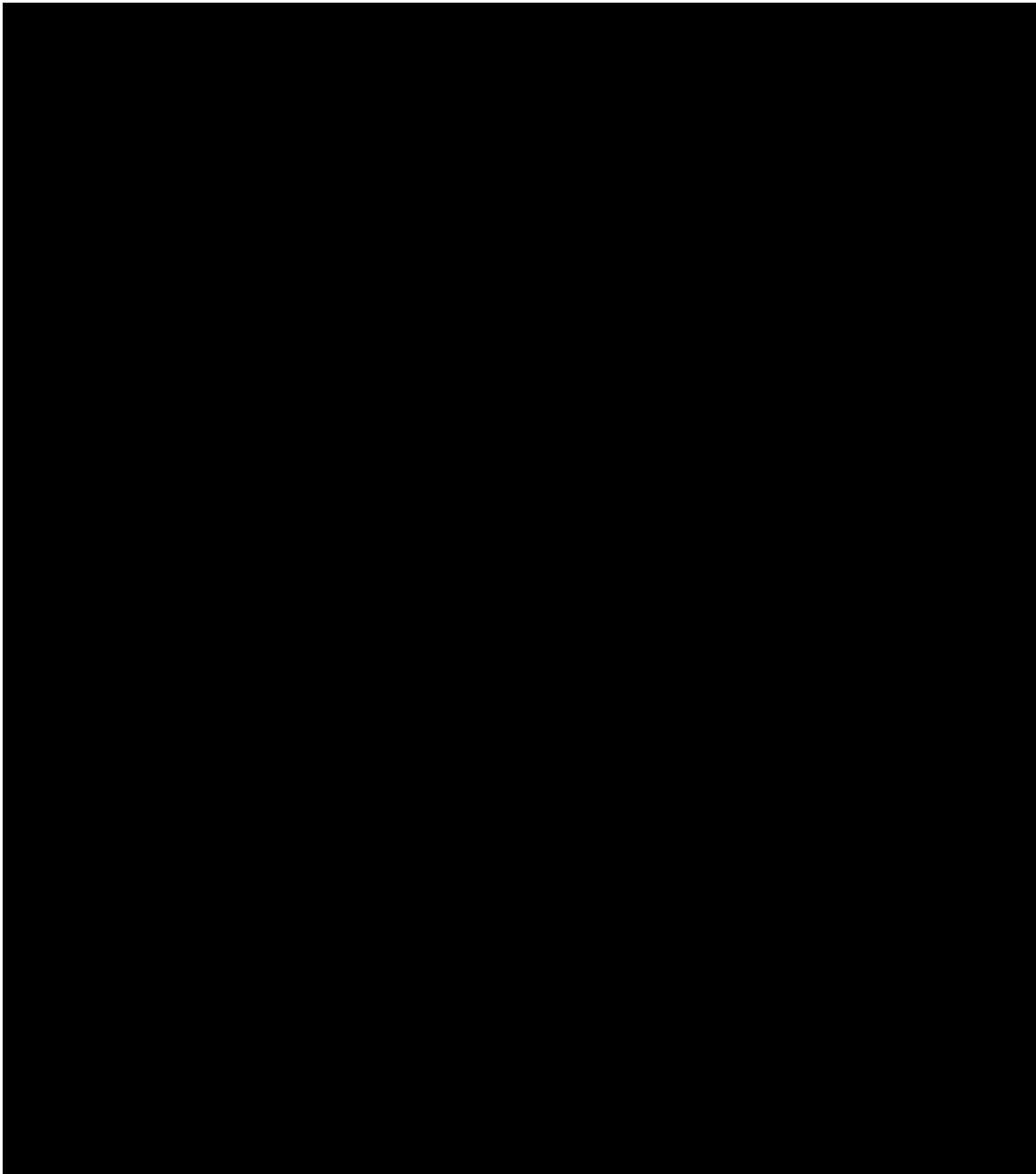
S

s 47F | facebook | Legal | 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

cid:image002.png@01D457FA.0AAB8380





From: s 47F
Date: 29 September 2018 at 2:35:25 am AEST
To: "angelene.falk@oaic.gov.au" <angelene.falk@oaic.gov.au>
Cc: s 47F
Subject: Important Update

Dear Ms Falk,

We wanted to alert you about an attack on our systems by an external actor that we are continuing to investigate. Please see the linked Newsroom Post for specific information, which will be issued shortly: <https://newsroom.fb.com/>

We are happy to schedule a call at your earliest convenience and answer any questions you may have.

Regards,

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

WARNING: The information contained in this email may be confidential. If you are not the intended recipient, any use or copying of any part of this information is unauthorised. If you have received this email in error, we apologise for any inconvenience and request that you notify the sender immediately and delete all copies of this email, together with any attachments.

From: s 47F
To: [Amie Grierson](#)
Cc: s 47F; [Melanie Drayton](#)
Subject: RE: Important Update [SEC=UNCLASSIFIED]
Date: Thursday, 4 October 2018 2:10:29 PM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image007.png](#)

Dear Amie,

As discussed yesterday, we can now provide the first breakdown for Australia to your Office with confidence, although please note this figure may change as our investigation progresses. Our engineering and data science teams have been working round the clock to make this information available as the data set of affected accounts was not a pre-defined term which we could query on the system, and therefore needed to be built. We expedited this work to ensure production of these figures as quickly as possible. Our priority however needed to be, and remains, securing the accounts. For the accounts in respect of which we have reset the access tokens as a precaution, the process was commenced on Friday morning (Syd time), and we have prioritised the numbers breakdown on completion of this process.

We are simultaneously working to determine whether these accounts were misused or any information accessed by the attacker, as well as assessing the potential risk to data subjects. We would be happy to continue to update you with more information as it becomes available, but we need to set expectations that obtaining clarity on what data was accessed is a considerably time-consuming process to ensure accuracy and complete analysis. We appreciate you will keep this information confidential as we continue to work on this analysis. Please note that our preliminary investigation indicates that credit card information would not have been visible to the attackers as we do not display the full credit card numbers in any account — not even to the account holder.

This number does not make any statement regarding whether accounts were subsequently accessed by the attacker, what data (if any) was exposed to the attacker, or other actions of the attacker in respect of the tokens. Our analysis of this continues.

236,000 is the number of accounts of Australian users that were the target of a URL call to “view as” during the window of 14 September 2018 – 28 September 2018 where we discovered an unexpected spike in 'view as' traffic (the “**Accounts viewed in ‘view as’ mode between 14 to 28 September 2018**”). For these accounts, we have reset the access tokens and as a result these users will have to log back in to Facebook, starting 29 September 2018. Again, at this stage of our investigation it is not possible to determine whether or not the attacker took any action on these accounts such as to access their information.

The date of 14 September 2018 is relevant, as that is when we believe this attack commenced, based on our investigations to date. Our analysis showed a large and unexpected spike in 'view as' traffic which we investigated and discovered this attack to obtain tokens.

For context in providing this information to you, we previously announced that the total number of accounts worldwide reflected in Accounts viewed in ‘view as’ mode between 14 to 28 September 2018 is approximately 50m.

We believe these figures to be an upper bound on the number of user Accounts viewed in ‘view as’ mode between 14 to 28 September 2018 that could have been affected. The numbers affected by the attack could indeed be significantly lower; we have sought to deploy an abundance of caution and adopted a conservative approach in order to maximise the safety of our users.

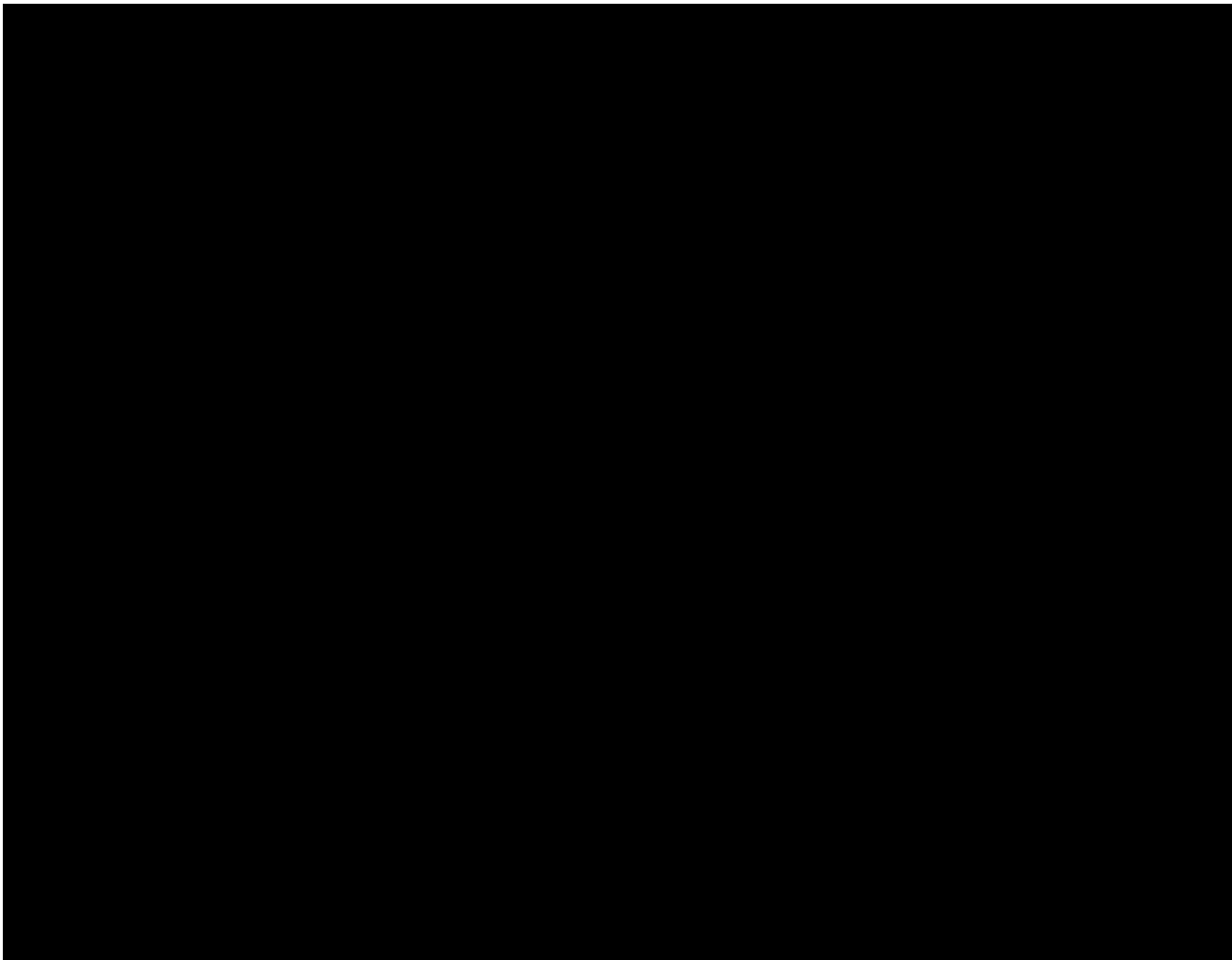
These numbers may change, and we would be happy to continue to update you with material further information. Please do not hesitate to contact me with any questions.

Kind regards,

s 47F | [facebook](#) | Legal | 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or

its contents.



From: s 47F [redacted]
Sent: Monday, 1 October 2018 2:29 PM
To: Amie Grierson <amie.grierson@oaic.gov.au>
Cc: s 47F [redacted]
[redacted] Melanie Drayton <melanie.drayton@oaic.gov.au>
Subject: RE: Important Update [SEC=UNCLASSIFIED]

Hi Amie,

To add to the below, both users and non users can also email Facebook directly via the alias datarequests@support.facebook.com. If you do share this with people (please feel free to do so) could you please ask them to reference the issue in the subject line i.e. please reference "Australia" and "Access Token" in the subject line, that will help our teams to track and prioritize reports. (People do not have to do this to receive a response but it would assist us in managing these requests).

Please do not hesitate to contact us with any questions.

Regards
s
4
7

From: s 47F [redacted]

Sent: Sunday, September 30, 2018 2:13 PM

To: 'Amie Grierson' <amie.grierson@oaic.gov.au>

Cc: s 47F

'Melanie Drayton' <melanie.drayton@oaic.gov.au>

Subject: RE: Important Update [SEC=UNCLASSIFIED]

Dear Amie,

Please see our responses to your questions below. If you have any further questions please do not hesitate to contact s 47F

1. Were any Australian Facebook accounts involved in the incident?

Our investigation is still in its early days and we're working hard to better understand these details. We don't know the location of all affected people. We also do not know if this was targeted to people from one particular country. We have so far found almost 50 million accounts that were affected. The security tokens for these accounts have already been invalidated to secure them. We've also taken the precautionary step of invalidating access tokens for another 40 million accounts that have been subject to a "View As" lookup. As a result, over 90 million people will now have to log back in to Facebook, or any of their apps that use Facebook Login. As we find more affected accounts, we will invalidate their access tokens — as well as the tokens of any more accounts we identify that have been subject to a "View As" lookup since July 2017.

2. If so, please advise how many Australians may have been impacted? *We will update you as soon as we know more details as to location of those affected.*

3. Whether at this stage you consider the incident to be an eligible data breach under the notifiable data breaches scheme? *At this stage we do not consider the incident to be an eligible data breach under the Australian notifiable data breaches scheme however we will continue to keep you and users informed about the incident and any developments.*

4. When did Facebook first become aware of the incident? *We became aware of the issue late on Tuesday 25th September 2018 (PST) (26th September 2018 (Syd))*

4. Any steps Facebook is taking to assess whether the matter is an eligible data breach for the purposes of the notifiable data breaches scheme, noting that eligible data breaches require notification to individuals and the OAIC under the scheme within statutory timeframes. *Our investigation is ongoing and we are continually assessing whether the incident is an eligible data breach under the notifiable data breaches scheme. We will continue to update both the OAIC and users with any developments.*

5. Whether there is specific information we might provide to individuals who may contact the OAIC with concerns about the incident, including how they can find out if they were impacted, what steps they should be taking to protect their privacy, and, if they wish to complain to Facebook about the incident, how they may do so. *Please alert them to the newsroom post <https://newsroom.fb.com/news/2018/09/security-update/> If they wish to contact Facebook directly they can do so through the channels as outlined in my email below.*

Kind regards

s

From: s 47F

Sent: Saturday, September 29, 2018 2:31 AM

To: 'Amie Grierson' <amie.grierson@oaic.gov.au>

Cc: s 47F

Melanie Drayton <melanie.drayton@oaic.gov.au>

Subject: RE: Important Update [SEC=UNCLASSIFIED]

Hi Amie,

Many thanks for speaking with me earlier today. As noted in the newsroom post (<https://newsroom.fb.com/news/2018/09/security-update/>), people with password issues can visit our [Help Center](#). If anyone wants to contact us for any other information relating to the recent notification they can also do this via the [Help Center](#) (the contact form is available at <https://www.facebook.com/help/contact/861937627253138>) and which is available even if the person is not a user of, or logged in to, Facebook. There is also a physical address available to all users:

Facebook, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Logged in users can also contact us through the Report a Problem tool (available if a user clicks on the question mark at the top right hand corner of a user's profile). Our privacy operations team are responding to the user questions that come through these (and other channels).

Please see attached images of the message that Facebook is using to notify affected users. As you would see, there is a "Learn More" button. Clicking on that button will lead to this [page](#). The notifications are rolling out globally now and will be live to all users by early next week. Please note, you may not see the notification the first time you log back in. We will provide further updates as the investigation develops.

For your convenience, below is a screenshot of the page. Please feel free to reach out to either myself s 47F for more information.

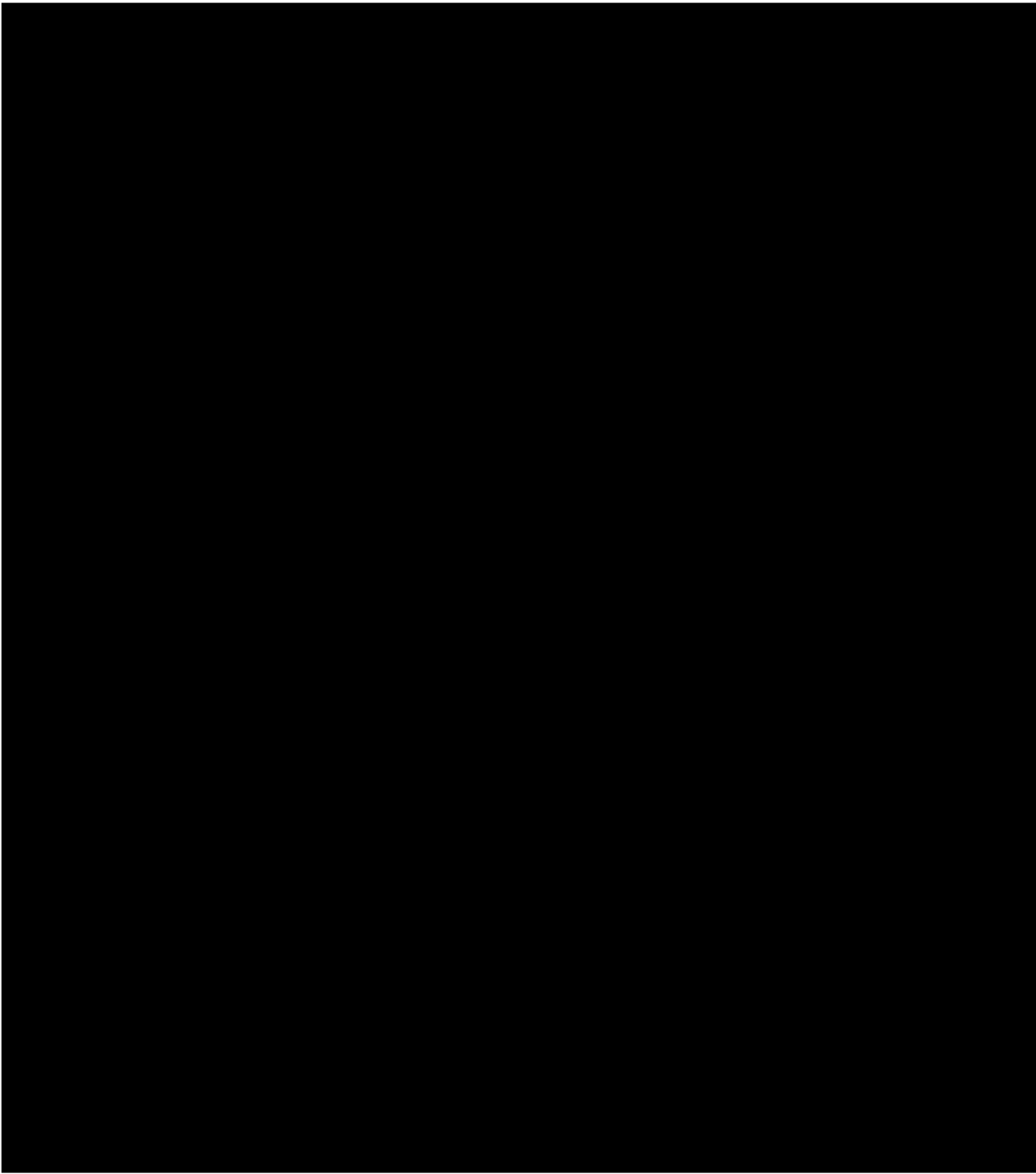
Kind regards,

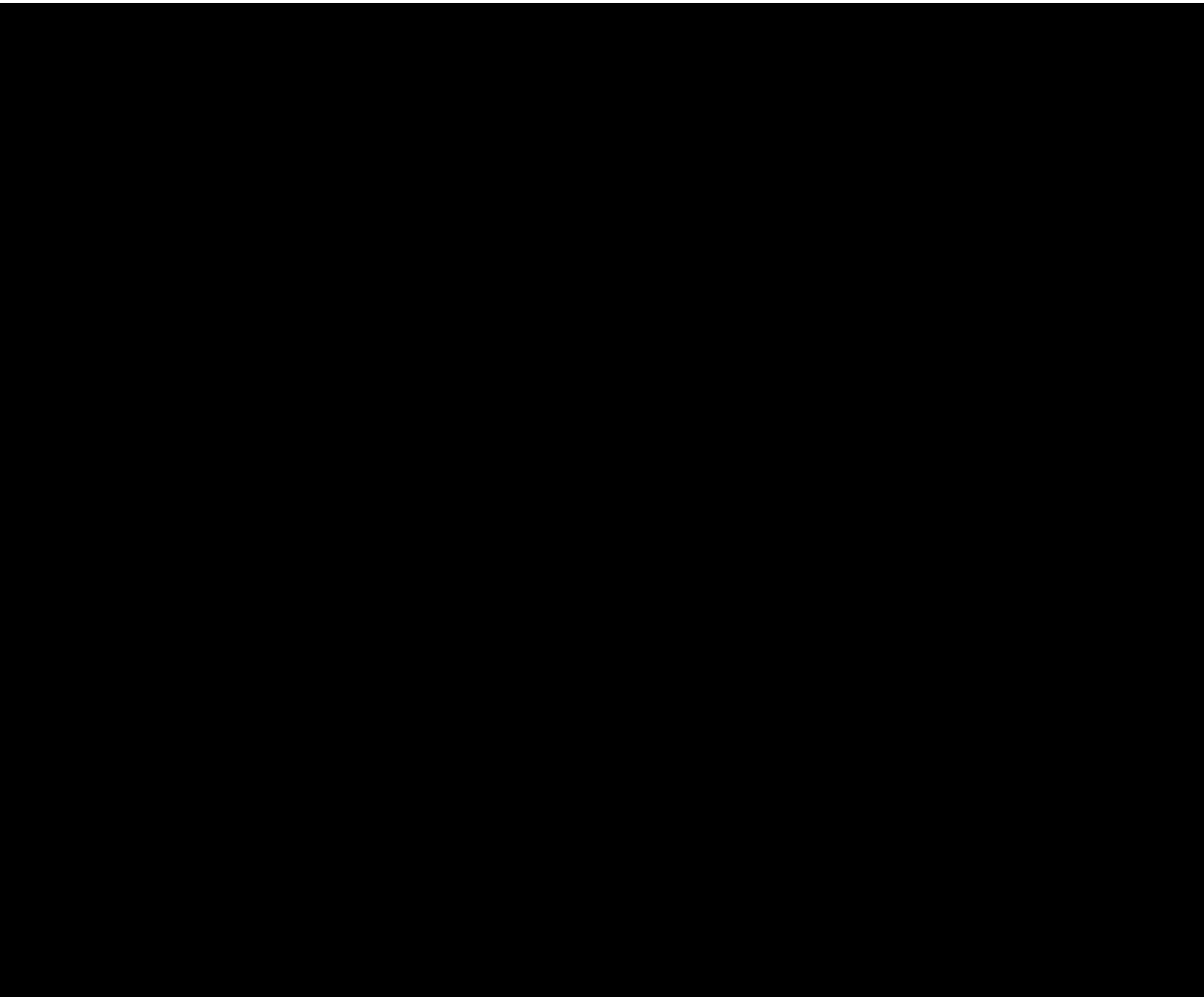
s
47F

-
| [facebook](#) | Legal | 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

cid:image002.png@01D457FA.0AAB8380





From: s 47F
Date: 29 September 2018 at 2:35:25 am AEST
To: "angelene.falk@oaic.gov.au" <angelene.falk@oaic.gov.au>
Cc: s 47F
Subject: Important Update

Dear Ms Falk,

We wanted to alert you about an attack on our systems by an external actor that we are continuing to investigate. Please see the linked Newsroom Post for specific information, which will be issued shortly: <https://newsroom.fb.com/>

We are happy to schedule a call at your earliest convenience and answer any questions you may have.

Regards,

s 47F | [facebook](#) | Legal, Privacy | 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

WARNING: The information contained in this email may be confidential.
If you are not the intended recipient, any use or copying of any part
of this information is unauthorised. If you have received this email in
error, we apologise for any inconvenience and request that you notify
the sender immediately and delete all copies of this email, together
with any attachments.

WARNING: The information contained in this email may be confidential.
If you are not the intended recipient, any use or copying of any part
of this information is unauthorised. If you have received this email in
error, we apologise for any inconvenience and request that you notify
the sender immediately and delete all copies of this email, together
with any attachments.

From: s 47F
To: [Amie Grierson](#)
Cc: s 47F
Subject: Access token update
Date: Friday, 12 October 2018 5:48:58 PM

Dear Amie,

I wanted to drop you a note to say that we know have some outstanding questions from you regarding our recent access token incident that are due today and I appreciate it is getitng close to COB in Australia. I wanted to assure you we will provide you with a more fulsome update tonight. I hope this does not cause any concerns but please do not hesitate to give me a call if you have any questions.

Regards,

s 47F | [facebook](#) | Legal | 47F

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

From: s 47F
To: Amie Grierson
Cc: s 47F; Melanie Drayton
Subject: Update re: Attack on Facebook Accounts
Date: Saturday, 13 October 2018 4:37:21 AM
Attachments: [OAIC Incident Update 13.10.2018.pdf](#)

Dear Amie,

We just published an update about our investigation into the attack that we announced on 28 September 2018. You can find more details in this Newsroom post: <https://newsroom.fb.com/news/2018/10/update-on-security-issue/>.

Please also find attached an update, which we are sending to you on a voluntary basis, in respect of the incident that we first raised with you on 28 September 2018 (PST).

As you know, we initially notified all users who we identified as potentially affected by the incident via an in-app update message on 28 September 2018 (PST). We will be issuing further user notifications about the incident shortly.

We have been working extensively to determine whether the potentially affected accounts were misused or whether any information was accessed by the attacker. Following further investigations (which are still ongoing) it appears information was obtained by the attacker.

We can confirm that following our investigation, we have revised down the overall 50m number for affected accounts globally to 29,088,724. We will send you the breakdown for Australia as soon as possible.

We have also created a new dedicated channel for responding to queries from affected users of this security vulnerability through our Help Center which will be included in our user notifications. We would appreciate it if going forward, the OAIC could refer any user queries it receives to that channel.

In addition to the information we have included in the attached update, we have some further detail that we would like to share with you about the incident. While we have already published some of this further information through our Newsroom, we would appreciate the OAIC keeping this confidential for now, while our investigations continue, as we do not want anything to adversely impact those investigations.

- Following further investigation, we believe that the vulnerability was introduced into Facebook's code on 12 July 2017 (PST). However, we believe that this attack, which led to access tokens being inappropriately accessed commenced on 14 September 2018 (PST), because we discovered (on 25 September 2018 (PST)) an unexpected spike in 'View As' traffic from that date. As previously indicated, we stopped this attack on 28 September 2018 (PST) by fixing the vulnerability.
- The vulnerability was the result of the interaction of three distinct bugs:
 1. 'View As' is a privacy feature that lets people see what their own profile looks like to someone else. 'View As' should be a view-only interface. However, for one type of composer (the box that lets you post content to Facebook) — specifically the version that enables people to wish their friends happy birthday — 'View As' incorrectly provided the opportunity to post a video.
 2. A new version of Facebook's video uploader (the interface that would be presented as a result of the first bug), introduced in July 2017, incorrectly generated an access token that had the permissions of the Facebook mobile application. This token was rendered in the HTML of the page.
 3. When the video uploader appeared as part of 'View As', it generated the access token not for the viewer, but for the user being looked up.

It was the combination of these three bugs that became a vulnerability. When using the 'View As' feature that permits a person to view his or her profile as a friend, the code did not remove the composer that lets people wish that person a happy birthday. The video uploader would then generate an access token when it should not have. When the access token was generated, it was not for the user but for the person being looked up. That access token was then available in the HTML of the page, which the attackers were able to extract. The attackers were then able to use that access token to access another account, performing the same actions and obtaining access tokens of friends associated with that account.

- As referred to in the update attached, we invalidated the access tokens of potentially affected accounts. This will have automatically protected any third-party developer using the Facebook software development kit (SDKs), save as explained below. However, as some developers who use our SDKs choose to use their own access tokens to validate users (rather than relying on Facebook's access token), and may not have re-checked the validity of the Facebook access token for each session, some third party apps could be maintaining their own logged-in sessions independently of Facebook access tokens. While, based upon our investigations to date, we do not believe the attack involved use of any compromised access tokens with third-party services, we have built a tool to enable such developers to identify the users of their apps who may have been affected by this issue, so that they can take protective action in the same way Facebook has done. This tool was launched on 4 October 2018.
- We have mobilised people across the company to help us determine what happened. We have a large team of engineers and data analysts working on this full-time, overseen by our Information Security Team. We have moved resources onto this effort from other areas in the business, as this takes critical priority in our business at the moment. Our teams have been working diligently to investigate the incident and understand how the attackers, once they had recovered access tokens, may have used those tokens to access Facebook systems and potentially collect information about users.

While we initially notified all users who we identified as potentially affected via an in-app 'important security update' message on 28 September 2018 (PST), which set out an explanation of the security incident, informed users that we had contacted law enforcement and explained the reasons and impact of resetting access tokens, we are planning to provide further communications to users potentially affected by the incident as soon as possible. This further communication will give users additional details of the incident, information about what further precautions they may wish to take and will provide a new dedicated channel for responding to queries from affected users. Users can find more information in this Newsroom post - <https://newsroom.fb.com/news/2018/10/update-on-security-issue/> - which we will update when we have more information.

We trust that the attached update and the further information in this email will address the matters raised in your letter to us on 5 October 2018 (AEST). Please let us know if you have any further queries.

Kind regards

S
47F

██████████ | facebook | Legal | 47F ██████████

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

Incident Update

Identity:

This update is issued by Facebook, Inc. (**Facebook**).

Description of the incident:

On September 25, 2018 (PST), we discovered that attackers had exploited a vulnerability caused by the complex interaction of three bugs in our system to obtain access tokens. Access tokens can be used, like a digital key, to request certain information through our platform. We acted quickly to secure the platform and began an investigation to determine if anyone's Facebook information was accessed and how many users were impacted.

To protect our users while we conducted an investigation, we invalidated the access tokens of almost 90 million accounts worldwide that may potentially have been impacted by the vulnerability.

Starting September 28, 2018 (PST), we notified all such users, explained why we did this and shared what we knew about the attack at that time. You can read more about [this incident and our initial response](#).

Based on our investigations to date, we now believe that between September 14 and 28, 2018 (PST), the attackers used the access tokens to obtain certain Facebook account information from our platform.

While we don't know if the attackers will use any of the information they accessed, we believe the main impact for affected users will be an increased likelihood that they will be the target for professional 'spam' operations.

We're actively working with law enforcement as we continue to investigate.

Information potentially affected by the incident:

Based on our investigation so far, our best estimate is that Facebook user data for up to **111,813** Australian users may have been accessed as a result of this incident. The data that may have been accessed, varies from case to case, across the following groups:

- 1 for an estimated 47,912 Australian users, the attackers may have obtained the following basic profile information:
 - Full name
 - Email address
 - Phone number (if there was one associated with the account)
- 2 for an estimated 62,306 further Australian users, in addition to the basic profile information potentially obtained in relation to the first group of users, the attackers may also have obtained the following information (to the extent that information was held in such fields following activity or provision of information by the user):
 - Username
 - First name used on the profile
 - Last name used on the profile
 - Name [nickname as set by the user on the profile (if any)]
 - Email address [primary email address associated with the account]
 - Phone [confirmed mobile phone numbers associated with account]
 - Gender [as set by the user on the profile]
 - Locale [language as picked by the user]
 - Relationship status [as set by the user on the profile]
 - Religion [as described by the user on the profile]

- Hometown [as set by the user on the profile]
 - Location [current city, as set by the user on the profile]
 - Birthday [as set by the user on the profile]
 - Devices [that are used by the user to access Facebook - fields include 'os' (e.g. iOS) and hardware (e.g. iPhone)]
 - Educational background [as set by the user on the profile]
 - Work history [as set by the user on the profile]
 - Website [list of URLs entered by the user into the website field on the profile]
 - Verified [this is a flag for whether Facebook has a strong indication that the user is who they say they are]
 - List of most recent places where the user has checked in [these locations are determined by the places named in the posts, such as a landmark or restaurant, not location data from a device]
 - Recent search queries on Facebook
 - Up to the top 500 accounts that the user follows
- 3 for a an estimated 1,595 further Australian users, in addition to the information potentially obtained in relation to the first two groups of users, the attackers may also have been exposed to additional information, including:
- Posts on their timeline
 - Their list of friends
 - Groups they are members of
 - The names of recent Messenger conversations.

Based upon what we've learned so far in our investigation, the attackers **did not** gain access to other personal information such as password information, identity documentation, financial information or payment card information.

Recommendations for affected users:

- We are in the process of planning a further communication to users potentially affected by the incident, giving users additional details of this incident and information about what further precautions they may wish to take, for example:
 - Being cautious of unwanted phone calls, text messages or emails from people users don't know.
 - That users' email address and phone number can be used to target them with spam or attempts to phish them for other information.
 - That, if users get a message or email claiming to be from Facebook, they can always review recent security emails to confirm if it's legitimate.
 - That other information can be used to send them personalized emails and messages that might be an attempt to scam them.

Users can find more details in this Facebook Newsroom post:
<https://newsroom.fb.com/news/2018/10/update-on-security-issue/>

From: s 47F
To: Amie Grierson
Cc: Melanie Drayton; Amanda Baird; Abby Aldana; s 47F
Subject: RE: Facebook data breach [SEC=UNCLASSIFIED]
Date: Saturday, 15 December 2018 6:38:52 PM

Dear Amie,

Thank you for your email. We are happy to provide information with regard to today's announcement regarding Facebook having discovered a bug that may have affected people who used Facebook Login to share their photos with third-party app developers. We have described the issue and the steps we have taken to address it on the Facebook Developer Blog (<https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/><<https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/>>). We also will be directly notifying people who have been affected.

We can confirm we do not currently believe the incident meets the requirements of the notifiable data breach reporting scheme. We hope to provide further information on your enquiries shortly.

Regards,

s
47F

From: s 47F
Sent: Saturday, December 15, 2018 2:34 PM
To: Amie Grierson <amie.grierson@oaic.gov.au>; s 47F
Cc: Melanie Drayton <melanie.drayton@oaic.gov.au>; Amanda Baird <amanda.baird@oaic.gov.au>; Abby Aldana <abby.aldana@oaic.gov.au>
Subject: Re: Facebook data breach [SEC=UNCLASSIFIED]

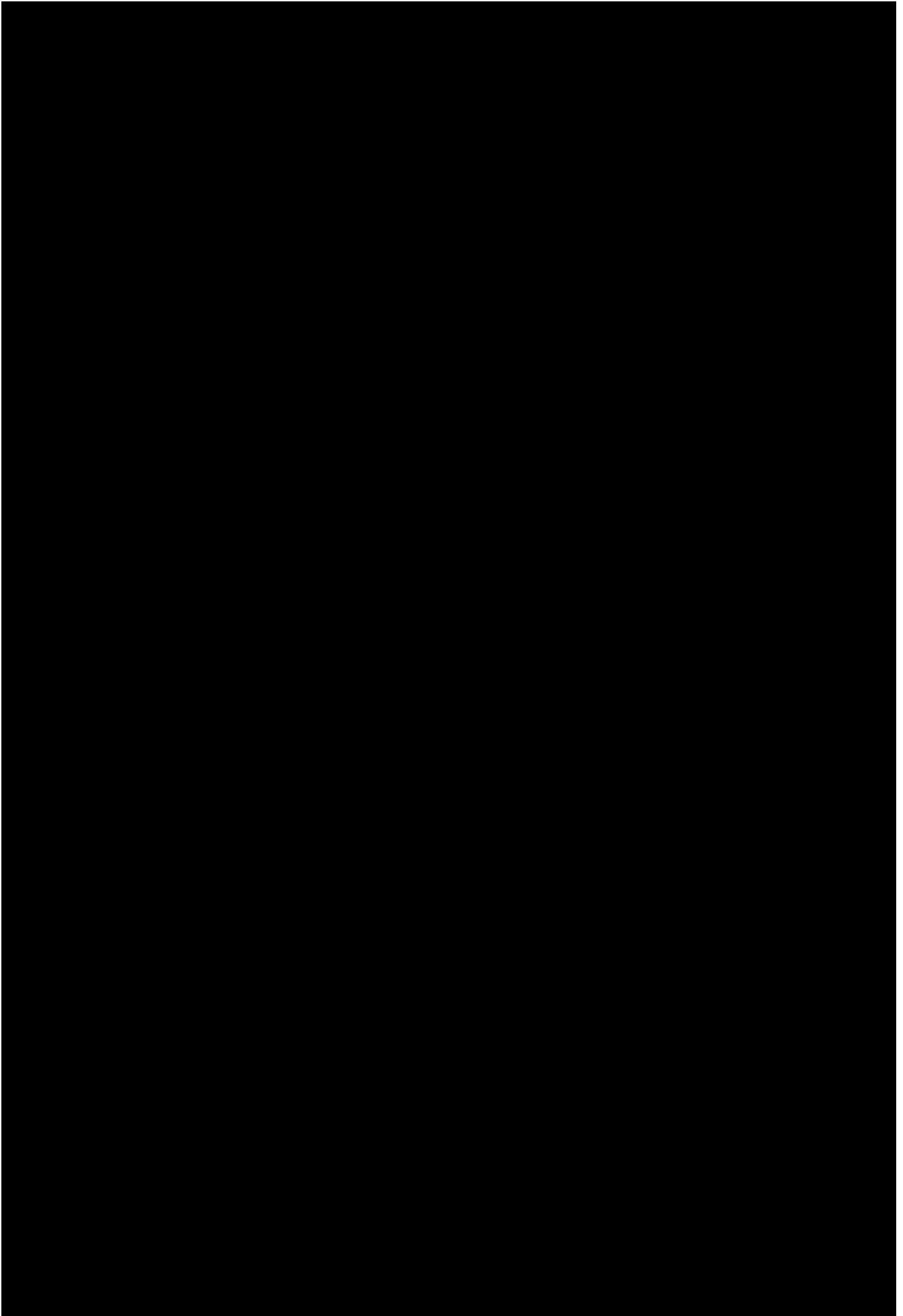
Hi Amie,

I wanted to acknowledge receipt of your emails. We will be reverting to you with responses to your questions shortly, however, I wanted to flag that it may not be today.

Kind regards,

s
47F





From: s 47F
To: [Amanda Baird](#); [Amie Grierson](#)
Cc: [Melanie Drayton](#); [Abby Aldana](#); s 47F
Subject: RE: Facebook data breach [SEC=UNCLASSIFIED]
Date: Wednesday, 19 December 2018 12:36:27 PM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)

Dear Amanda and Amie,

My apologies for not responding to you sooner. Please see the answers to your queries below:

1. The number of Australian users affected by the bug is 68016. Please note that this numbers are a ceiling, because its include all users who may have experienced the bug. We cannot determine with precision whether specific photos were actually accessed by third party apps. We anticipate that the number of actually concerned users is much lower.
2. Facebook begun notifying individuals on Monday, December 17 (PST).
3. The developer notices were also sent on Monday, December 17 (PST). The tool for developers to use is live and was live at the point the notices were sent.

Please do not hesitate to contact s 47F or myself with any further queries.

Regards,

s
47F





From: s 47F

Sent: Saturday, 15 December 2018 6:38 PM

To: Amie Grierson <amie.grierson@oaic.gov.au>

Cc: Melanie Drayton <melanie.drayton@oaic.gov.au>; Amanda Baird <amanda.baird@oaic.gov.au>; Abby Aldana <abby.aldana@oaic.gov.au>; s 47F

Subject: RE: Facebook data breach [SEC=UNCLASSIFIED]

Dear Amie,

Thank you for your email. We are happy to provide information with regard to today's announcement regarding Facebook having discovered a bug that may have affected people who used Facebook Login to share their photos with third-party app developers. We have described the issue and the steps we have taken to address it on the Facebook Developer Blog (<https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/> <<https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/>>). We also will be directly notifying people who have been affected.

We can confirm we do not currently believe the incident meets the requirements of the notifiable data breach reporting scheme. We hope to provide further information on your enquiries shortly.

Regards,

s
47F

From: [REDACTED]

Sent: Saturday, December 15, 2018 2:34 PM

To: Amie Grierson <amie.grierson@oaic.gov.au>; s 47F

Cc: Melanie Drayton <melanie.drayton@oaic.gov.au>; Amanda Baird <amanda.baird@oaic.gov.au>; Abby Aldana <abby.aldana@oaic.gov.au>

Subject: Re: Facebook data breach [SEC=UNCLASSIFIED]

Hi Amie,

I wanted to acknowledge receipt of your emails. We will be reverting to you with responses to your questions shortly, however, I wanted to flag that it may not be today.

Kind regards,

S

