Report of investigation into AMEX

Privacy Commissioner's foreword

Insider security risk remains a significant, yet frequently overlooked, threat to organisations, and to the individuals whose personal information they are entrusted with. Risk arises when individuals with legitimate access to systems and personal information misuse that access in ways that compromise privacy or security.

As outlined in this report, I recently made a determination in 'BAM' and American Express Australia Limited (**AMEX**) in which I explored the issue of insider security risk within a financial institution. The determination examined circumstances in which an AMEX employee's authorised access to relevant systems enabled them to view a range of information about AMEX customers, including travel and hotel bookings, and financial transactions. A former AMEX customer subsequently alleged to both AMEX and my office that the employee had accessed their account and personal information for purposes outside of legitimate business purposes.

I concluded that AMEX had failed to meet its obligation under Australian Privacy Principle (**APP**) 11.1 to take reasonable steps to protect the information it held from unauthorised access, particularly from insider security risks. The determination also considered AMEX's complaint handling procedures as against the requirements of APP 1.2.

This report details findings of that determination and highlights broader implications for entities subject to the *Privacy Act 1988* (Cth) (**Privacy Act**). It underscores the need for regulated entities to implement a suite of measures, including appropriate technical controls, to mitigate insider security risk and protect personal information from unauthorised access.

Section 33C of the Privacy Act empowers me to release information where doing so is in the public interest. I have decided to publish this report, which summarises my determination because of the educative value in disseminating the OAIC's findings against AMEX for the broader regulated community.

Introduction

Insider security risk refers to the threat that arises when individuals with authorised access to an organisation's systems and data, misuse that access in ways that compromise privacy or security. Risk is not confined to harm suffered by an organisation itself - it also extends to customers, whose personal information may be viewed, disclosed or otherwise used inappropriately by an employee, contractor or other authorised user.

The risk that staff may seek access to personal information on their employer's systems for improper purposes is an unfortunate reality. Such conduct can occur in a range of contexts, including financial fraud, domestic and family violence, or political, military or corporate espionage. The risk is heightened in sectors that store large volumes of personal information, such as the financial services sector.

Entities that hold personal information must ensure that robust controls are in place to prevent unauthorised internal access. Effective management of insider security risk requires more than organisational policies or staff training – it also requires the implementation of technical controls as appropriate such as access and action logging and an ability to restrict access to specific customer information.

The following section examines insider security risk through the lens of:

- APP 11.1, which requires organisations to take reasonable steps to protect personal information from misuse and unauthorised access, use or disclosure; and
- APP 1.2, which requires organisations to take reasonable steps to implement practices, procedures and systems that will enable them to comply with the APPs (APP 1.2(a)) and deal with complaints and enquiries about their APP compliance (APP 1.2(b)).

This report highlights lessons from a recent determination to illustrate how these obligations can be applied in practice.

Relevant provisions of the Privacy Act

APP 11.1 - Security of Personal information

APP 11.1 requires an APP entity to take such steps as are reasonable in the circumstances to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Reasonable steps include technical and organisational measures. Technical measures include protecting personal information by implementing technological controls and physical measures relating to software and hardware. Organisational measures involve implementing policies, processes and procedures to protect the security of information.

The Federal Court of Australia (**Court**) has provided guidance on the approach to be taken to determine if steps taken were reasonable in the circumstances,[1] observing that the focus must always be on whether the steps that were taken, in their totality, were reasonable.[2] This requires consideration of whether the steps that were taken to protect personal information were commensurate to the risks presented in the relevant circumstances.[3] The obligation will differ depending on the complexity of the entity's business and the procedures within the entity; is not capable of being discharged simply by delegating it to another entity; and requires a holistic analysis, considering the full framework of the entity's systems, policies and procedures.[4]

Reasonable steps will depend on the circumstances. In all cases, reasonable steps should include taking steps and implementing strategies in relation to:

- governance, culture and training;
- internal policies, procedures and systems;
- ICT security; and

[1] Australian Securities and Investments Commission v Firstmac Ltd [2024] FCA 747; Australian Securities and Investments Commission v R M Capital Pty Ltd [2024] FCA 151.
[2] Australian Securities and Investments Commission v R M Capital Pty Ltd [2024] FCA 151, [80].
[3] Australian Securities and Investments Commission v R M Capital Pty Ltd [2024] FCA 151, [85].
[4] Australian Information Commissioner v Australian Clinical Labs Limited (No 2) [2025] FCA 1224 at [51].

- technical measures including action logging and an ability to restrict access to specific customer information.

APP 1.2 - Open and transparent management of personal information

APP 1.2 requires an APP entity to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities that will:

- ensure the entity complies with the APPs and any binding registered APP code (see Part IIIB); and
- enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs and any binding registered APP code.

The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The obligation is a constant one, and also subject to a 'reasonable steps' test, meaning that the steps required to be taken by the entity will depend on circumstances that include the nature of personal information held, the possible adverse consequences for an individual if their personal information is not handled as required by the APPs, the nature of the APP entity (including its size and resources), and the practicability of implementing steps.

Determination – 'BAM' and American Express Australia Limited

Background

The complaint arose in circumstances in which the complainant alleged access to the complainant's personal and financial information held on AMEX's systems by an employee of AMEX with whom the complainant had formerly had a personal relationship.

The OAIC's investigation of the complainant's privacy complaint involved an inquiry into the technical and organisational measures that AMEX had in place to prevent any unauthorised access to personal information, as required by APP 11.1, including steps to prevent unauthorised access by AMEX's staff.

This determination underscores the obligations entities bear to consider and mitigate insider security risks as part of their organisational and technical measures to secure personal information from misuse and unauthorised access. It also considers how entities should handle privacy complaints that pertain specifically to employees of an entity.

Factual circumstances

The complaint was against AMEX, a globally integrated financial services and payments company. AMEX holds an Australian Credit Licence and an Australian Financial Services Licence. The products and services offered by AMEX include, but are not limited to, credit and charge card products, travel and lifestyle services and travel insurance. The factual circumstances are referable to the period in which events took place and relevant responses to the OAIC investigation.

The complainant had a personal relationship with an employee of AMEX (**employee**).

In the course of their employment, the employee was required to use certain ICT systems and had access to 5 ICT systems containing personal information of the complainant. These systems will be referred to as System 1, System 2, System 3, System 4 and System 5 (together, **Relevant Systems**). Access to the Relevant Systems enabled the employee, in their role to view a range of information about AMEX's customers, including customer names, travel and hotel bookings, rewards information and financial transactions.

The complainant alleged that, during the relationship and after its breakdown, the employee accessed, used and disclosed the complainant's account information, including their personal information, in a range of contexts and for purposes outside of legitimate business purposes. The complainant asserted that they became aware of such access and disclosure when, in conversation, the employee made reference to information they had gleaned through access to the complainant's personal information held on AMEX's systems. The complainant noted that when the employee offered information about the complainant's transactions or points, the complainant did not request this information or acknowledge it as helpful. Based on these interactions, the complainant understood that the employee had accessed their account.

With respect to the employee's access to the complainant's records, AMEX submitted this was not materially in dispute, and that the employee had confirmed accessing the complainant's personal information. However, AMEX did not have account-level access logging uniformly enabled across the Relevant Systems that contained the complainant's personal information; that is, it did not record each instance that an employee accessed a specific customer record. As a result, AMEX could not evidence whether the employee accessed the complainant's account on further occasions.

AMEX's handling of complaint to AMEX

In the first instance, the complainant made a written complaint to AMEX alleging the employee improperly accessed their account on multiple occasions. In the complaint and in subsequent communications, the complainant raised certain allegations against the employee directly. After receiving the complaint, AMEX escalated the matter internally, and took steps to investigate, including reviewing the employee's access logs (where available); undertaking interviews and meetings with relevant staff; and reviewing AMEX's internal policies and training materials.

Compliance with APP 11.1

In determining whether AMEX breached APP 11.1, the OAIC's investigation focussed on what steps AMEX took to protect the personal information it held from insider security risks, and whether those steps were reasonable in the circumstances to protect that information from those risks.

The OAIC adopted the following analytical approach to determine whether the steps that AMEX took were reasonable in the circumstances to protect the complainant's personal information from unauthorised access by employees:

a) What are the relevant circumstances?
b) What steps were taken by AMEX to protect the complainant's personal information it held from insider security risks?

c) Were the steps taken by AMEX, in their totality, commensurate to the insider security risks, in relation to the complainant's personal information it held?

Factors that may be relevant to assessing whether particular steps were reasonable in the circumstances may include the degree of difficulty or practicability of any given step, and the costs associated with them. Additionally, a step may be reasonable but unnecessary because an APP entity is taking other steps commensurate to the risk, to which the proposed step adds nothing.

What are the relevant circumstances?

In accordance with the APP Guidelines,[5] the OAIC considered the following matters to be relevant to determining whether the steps taken by AMEX were reasonable to ensure the security of the complainant's personal information:

a) **Amount and sensitivity of personal information held**: AMEX holds vast amounts of personal information on its customers. Australia is a jurisdiction that represents a significant portion of AMEX's billed business. AMEX holds personal information across the Relevant Systems which hold, or historically held, the personal information of the complainant. AMEX advised that the types of personal information it holds for its customers may include name and contact details, bank details, account and transaction information, travel booking information and credit limit information. The granular nature of transaction and travel data is capable of revealing detailed information about an individual's habits, movements and personal circumstances which, if disclosed, could in certain circumstances result in serious harm.
b) **Potential harm to individuals of unauthorised access:** Employees of AMEX have access to granular transaction data, travel bookings, location information and, in some cases, health-related information. Unauthorised access to such information by an employee has the potential to facilitate a range of potential harms, including financial fraud, identity theft, physical harm or intimidation.
c) **Size and sophistication of APP entity:** AMEX is part of a highly sophisticated entity, being a global financial services and payments company.
d) **Cybersecurity environment and history:** Prior to the events that are the subject of this determination, AMEX's group (internationally) had experienced the realisation of an insider security risk – that is, an insider threat incident involving the wrongful access of customer data by an employee. Accordingly, in 2019, AMEX's group issued data breach notifications to affected cardholders after an employee was found to have wrongfully accessed customer account information – including full names, card account numbers, physical and billing addresses, dates of birth and Social Security numbers – in an attempt to conduct fraudulent activity, including opening accounts at other financial institutions.

What steps were taken by AMEX to protect the complainant's personal information it held from insider security risks?

The OAIC's investigation considered steps AMEX had in place to assess whether it met the requirements of APP 11.1, including technological and organisational measures during the period of 14 January 2022 (the date the complainant advises that they commenced a personal

[5] Australian Privacy Principles guidelines | OAIC

relationship with the employee) to 29 May 2025 (the date a preliminary view was sent to the complainant and AMEX), which captured the period in which the employee accessed the complainant's personal information (**Relevant Period)**.

AMEX submitted that it had the following controls and processes in place to protect the personal information it holds from unauthorised access:

a) A system to manage role-based access to systems and applications, as well as supporting policies, standards and procedures, which limits employee access subject to their role and having a legitimate 'business need to know';
b) risk management policies and technology standards relating to cyber security and privacy, including a Privacy Risk Assessment Standard and a Logging Management Standard;
c) staff training on Information Access Management, including training on data security, privacy and how information access and entitlements should properly be used;
d) a Privacy Risk Assessment Standard, under which privacy risk assessments are conducted in respect of any activity that involves the processing of personal information;
e) Identity and Access Management Leader Access Reviews of current employee information access entitlements to determine if access entitlements associated with designated ICT programs should be retained;
f) cyber security reviews, assessments and business unit audits;
g) a Code of Conduct which, among other things, governs employee conduct with respect to access to customer information;
h) an End Point Protection Standard, which requires detection, prevention, removal and recovery controls to protect information against malicious activity; and
i) a Global Servicing Group (**GSG**) Monitoring program, which deploys analytical risk indicators to detect out-of-pattern or excessive access by frontline staff to card member accounts.

AMEX's Code of Conduct, inter alia:

a) requires that employees only collect, use, view and access personal data where there is a legitimate business need to do so;
b) requires employees to avoid conflicts of interest, including situations where a staff member might use their position, or information acquired through their position, in a way that creates a conflict of interest between their personal interests and the interests of AMEX or its customers;
c) prohibits employees from sharing information about AMEX's customers with friends or family or unauthorised individuals; and
d) requires employees to disclose all conflicts and potential conflicts of interest using its Code of Conduct Disclosure Portal, noting conflicts can arise inadvertently, due to business or personal relationships with customers or suppliers.

Were the steps taken by AMEX, in their totality, commensurate to the insider security risks, in relation to the complainant's personal information it held?

The steps AMEX took went some way toward the reasonable steps required by APP 11.1, and it took steps to respond to the actions of the employee. However, AMEX did not take such steps as were reasonable in the circumstances to protect the personal information it held.

In reaching this conclusion the Commissioner had regard to the circumstances and AMEX's group's prior experience of an insider threat incident, which required a higher standard of preventative controls.

In particular, AMEX failed to implement appropriate, uniformly applied technical and organisational measures to address insider security risks posed by its staff. The Commissioner acknowledged AMEX's submission that its GSG Monitoring program deployed analytical 'scanners' to detect out-of-pattern access, including access to prominent accounts or access without a corresponding customer call. However, AMEX admitted this program did not extend to the employee's team during the period in which the employee accessed the complainant's personal information. This failure is particularly significant given AMEX was on notice of the need for uniform monitoring coverage across all frontline teams having experienced the previous insider threat incident.

As a result of this critical gap in coverage, AMEX's systems remained vulnerable to misuse or unauthorised access by employees, including in relation to the accounts of their family, friends, or prominent individuals. In circumstances in which the financial sector was the second highest-reporting industry for notifiable data breaches during the period of the data breach, AMEX should have taken further steps to mitigate the risks of unauthorised access to personal information held in its systems. The Commissioner was of the view that there were other steps that AMEX could reasonably have taken to protect the personal information it held from insider security risks, and in particular the risk of unauthorised access by its employee(s), namely:

a) uniform account-level access logging across all Relevant Systems;
b) restricting access to certain customer records;
c) implementing Just in Time access; and
d) prohibiting employee access to the customer accounts of their friends and family.

Logging of action and access events

AMEX provided a copy of its Logging Management Standard, which states that 'logging must be enabled to capture activities related to support, performance and security on systems and applications'. AMEX's Logging Management Standard is an internal technology standard that applies to AMEX's systems and applications. AMEX submitted that the requirements for logging capability set out in the standard apply to all systems and applications.

At the commencement of the OAIC's investigation, AMEX described the following categories of logging in its ICT systems:

a) **Access Logging:** logging access to an individual record at a customer account level.
b) **System Access Logging:** logging access to the system or application (i.e. a time/date stamp when an employee opens or closes a system).
c) **Action Logging:** logging write-access or actions taken in respect of an individual record.

In this context, a critical distinction arises between account-level Access Logging – which records each instance of an employee accessing a specific customer record – and System Access Logging, which records only when an employee opens or closes an application. As discussed below, the absence of account-level Access Logging on a system means that browsing of customer records within that system cannot be detected, traced or audited.

The investigation focused on the five Relevant Systems on which the complainant's personal information was held. In particular, the investigation examined whether account-level Access Logging was uniformly enabled across the Relevant Systems during the Relevant Period.

AMEX submitted that logging capability is achieved through a combination of system-specific and authentication-based mechanisms. AMEX set out the logging arrangements in operation for four of the Relevant Systems as set out below. AMEX advised that System 3 replaced the fifth ICT system the subject of this investigation – known as System 4 - in June 2022.

	Access Logging	**System Access Logging**	**Action Logging**
System 1	Enabled	Enabled	Enabled
System 2	Enabled (introduced 2023)	Enabled	Enabled
System 3	None	Enabled	Enabled
System 5	Enabled	Enabled	Enabled

AMEX later introduced and detailed another type of logging. AMEX stated that this type of logging operates as a substitute for Access Logging on System 1 and System 3. According to AMEX, this type of logging usually requires a user to authenticate a caller by correctly answering verification questions before access to a customer profile is granted. If either the caller, or the employee entering the responses, answers incorrectly, access is not granted to the customer profile. AMEX also described an alternative authentication pathway. In this mode, an employee may access customer records without answering the verification questions. This appears to be a workaround that may render as ineffective the former type of logging as a substitute for access controls on customer records.

AMEX stated that the formerly described type of logging creates the equivalent of access control logs for System 1 and System 3. However, it is not clear whether this is so, particularly as AMEX's previous submissions did not describe these systems as having this level of logging capability. Further, the existence of the alternative authentication pathway raises access control concerns as it appears that the employee had this entitlement. This appears inconsistent with AMEX's assertion that this type of access is only granted where there is valid business need or justification.

AMEX's own submissions confirm that account-level Access Logging was absent from System 2 during the Relevant Period and introduced only after the events the subject of the complaint. This gap is significant because System Access Logging and Action Logging do not record when an employee accesses a specific customer account within a system – only account-level Access Logging does. This is at odds with AMEX's Logging Management Standard, which requires that logging is enabled to capture all activities relating to support, performance and security of systems and applications.

AMEX submitted that there are fundamental differences in 'System Characteristics', including system architecture, data flow complexity, and business function, that must be considered individually to determine if its logging was reasonable. While the technical environment across the Relevant Systems is not uniform, these characteristics do not negate the necessity of account-level Access Logging to address the inherent privacy risk of unauthorised access.

Regardless of an entity's specific system architecture, where it holds personal information in AMEX's circumstances, enabling both action and account-level access logging is a reasonable step for an entity to take. This is reflected in AMEX's own Logging Management Standard and is also reflected in the United States National Institute of Standards and Technology Cybersecurity Framework (NIST Cyber Security Framework) control PR.PT-1, being the requirement that audit/logs records are determined, documented, implemented, and reviewed in accordance with policy.

The distinction between account-level Access Logging and System Access Logging is not in dispute. In its submissions dated 15 December 2023, AMEX explained: 'Access logging refers to the logging at a customer account level. That is, each time an employee accesses a customer account, it is logged. System access logging refers to logging at the system level. That is, each time an employee opens and closes a system, it is logged with a time/date stamp. However, this does not include a time/date stamp for each instance of customer account access within the system'. It follows that System Access Logging cannot show which customer records an employee accessed within a system, or when. The absence of account-level Access Logging on System 2 during the Relevant Period therefore meant that any browsing of customer records within that system – including any unauthorised access – could not be detected, identified or traced through that system's logging alone. While Action Logging records write-access events, it does not capture read-only access to a customer account. An employee who accessed – but did not modify – a customer record on System 2 during the Relevant Period would therefore have left no account-level trace in that system.

These limitations are relevant to AMEX's investigation of this complaint. For example, AMEX stated that the employee's unauthorised access of the complainant's personal information was an isolated incident, flowing from a personal arrangement between the complainant and the employee.

However, while AMEX was able to identify the specific occasions when the employee accessed the complainant's records on the Relevant Systems that had account-level Access Logging enabled during the Relevant Period (System 1 and System 5), it could not provide the same assurance with respect to the remaining Relevant Systems.

AMEX submitted that its 'multiple layers of monitoring' and 'System Access Logging' would likely have detected similar incidents had they occurred. However, System Access Logging cannot show which customer records an employee accessed within a system, or when; it therefore cannot detect or evidence unauthorised browsing of customer records.

AMEX also referred to three further controls as supplementing its logging capability.

- First, on its Conduct Risk Governance program, which AMEX describes as relying on random sampling and 'risk-based triggers' – such as customer complaints and targeted scanners – to identify instances of misconduct: The Commissioner did not accept that this constitutes an adequate substitute for account-level Access Logging. Random sampling does not provide continuous or comprehensive visibility of employee access to customer records; it is a reactive and selective mechanism that, by its nature, may fail to detect unauthorised access that does not generate a complaint or trigger a scanner.
- Second, 'Application Health Scores' – annual scorecard assessments of application security risk criteria, which may include logging criteria: These are an administrative governance tool; they are not a real-time or systematic record of who accessed which customer account at what time.

- Third, quarterly server log coverage undertaken to ensure application compliance with logging requirements: This too is a periodic compliance check, not a continuous record of customer account access events.

None of these controls substitutes for the technical, preventative function of account-level Access Logging, which creates a contemporaneous, comprehensive and auditable record of all access to customer accounts.

Furthermore, AMEX's primary monitoring program – the GSG Monitoring program – did not extend to the employee's team during the Relevant Period. In the absence of rigorous and uniform account-level Access Logging across all Relevant Systems, AMEX was not in a position to conclude that similar breaches had not occurred in the past. Should these limitations remain unaddressed, they will continue to impede AMEX's ability to properly investigate and respond to privacy or security incidents affecting its systems in the future.

In terms of the impact on AMEX, the Commissioner was not satisfied that implementing account-level Access Logging across all Relevant Systems would impose an unreasonable burden, having regard to AMEX's size, resources, the sensitivity of the information it holds, and the adverse consequences for individuals where their personal information is not being protected from unauthorised access. It was noted in this regard that AMEX had already implemented account-level Access Logging on System 1 and System 5 during the Relevant Period. AMEX forms part of a global financial services and payments company with staff worldwide. The granular nature of transaction data and travel information AMEX holds in its systems has the potential to reveal information about an individual's location and movements, as well as other sensitive personal information. Accordingly, AMEX's failure to implement access and action logging on the Relevant Systems may have serious consequences for individuals. These potential consequences include financial fraud, identity theft, domestic and family violence, and physical harm or intimidation.

Restricting access to certain customer records

AMEX explained that staff are granted privileges to access its systems where required for their role. However, once these role-based privileges are granted, employees can generally access any customer record within those systems. In relation to the five Relevant Systems, AMEX submitted that it does not limit access to specific customer records and was unable to practically restrict its employees from accessing certain data within four of them.

AMEX referred to complementary systems and controls, including training, role-based controls, system monitoring, access logging, and incident prevention, detection, and response processes to protect the personal information it held. AMEX said it had a range of additional policies and standards which support these controls, including its Code of Conduct, records management policy, privacy risk policy, and information security management policy.

Rather than technical controls, AMEX relies on its policies, hiring practices, and training. This includes ensuring employees understand "need to know" principles and training regarding access to the accounts of family, friends, and celebrities. However, AMEX's submission that it 'is unable to practically restrict' access to certain records highlights a vulnerability for customers, particularly those who are high-profile or vulnerable individuals.

AMEX subsequently submitted that it does have the capability to restrict access by suspending an employee's system access or removing specific entitlements. However, AMEX does not appear to have exercised any such capabilities in respect of the employee, which calls into question whether such capabilities represent an effective protection. If an entity possesses the capability to restrict access but fails to exercise that capability when put on notice of a specific, heightened privacy or security risk, it cannot point to the existence of the capability as evidence that it has taken reasonable steps to secure personal information.

Developing technical controls or security measures to support individual or personalised access restrictions was, in the circumstances, a reasonable step for AMEX to take. While the practical implementation of such a step is complex, there was no evidence that it was not a reasonable requirement given AMEX's substantial resources and the sensitive nature of the information. Moreover, the counterbalancing controls identified by AMEX did not mitigate the specific risk of unauthorised access in this case.

Just in Time Access

'Just-in-time access' (**JIT**) and similar processes prevent customer support agents from accessing customer records without a specific, time-bound trigger, such as active authentication from the customer. This serves the dual purpose of verifying the customer's identity and ensuring the agent only accesses records for a legitimate, authorised purpose.

This differs from the access currently afforded to AMEX's employees where, once a relevant access privilege is granted by AMEX, employees maintain broad access to customer records within those systems, especially if they are granted an alternative authentication pathway.

AMEX concluded the incidents in this case were the result of the employee acting in breach of policies, noting 'the issues … were caused by a sole actor.' AMEX further submitted that two of its systems (System 1 and System 3) have authentication protocols "similar" to JIT and that its GSG Monitoring program includes scanners to detect 'Accessing Personally Identifiable Information (PII) Without a Call'. However, the case highlights a persistent vulnerability: staff maintained the technical ability to access personal information without a legitimate purpose, and this conduct went undetected by AMEX at the time of the breach.

AMEX submitted that implementing JIT access for systems like System 5 and System 2 is 'neither practicable nor reasonable' and that requiring customer contact for every access would be 'burdensome'. While there are undoubtedly operational complexities, the 'reasonable steps' required under APP 11.1 must be commensurate to the risk. AMEX's reliance on 'scanners' designed to detect access to accounts without a corresponding customer call – which did not extend to the employee's team - was an insufficient protection.

Had AMEX had JIT access in place at the time of the 2022 events, it would have been more likely to prevent any instances of unauthorised access. This was a step that AMEX could have taken to protect personal information from unauthorised access.

Prohibiting employee access to friend and family accounts

The investigation also considered AMEX's management of security risks, and the risk of unauthorised employee access to customers' personal information.

AMEX's group's prior experience of an insider threat incident is relevant to this assessment: it demonstrated that the risk of an employee misusing access to customers' information for personal purposes was not a speculative or remote possibility but a risk that had already materialised within AMEX's group.

AMEX's Code of Conduct requires employees to only use personal information for a legitimate business purpose and not to share information about its customers with friends, family, or unauthorised individuals. It also requires employees to avoid conflicts of interest. AMEX also submitted it has a longstanding policy position that staff are not permitted to access or service family accounts.

However, the Code of Conduct AMEX produced to the OAIC in the investigation does not explicitly state that an employee is prohibited from accessing the accounts of friends and family members. The absence of these explicit prohibitions meant that there was no clear policy framework to trigger an immediate restriction of the employee's access even if AMEX became aware of the 'personal arrangement' between the employee and the complainant.

Had AMEX developed clearer guidance around internal security risks and employees accessing the personal information of friends or family members, this may have underpinned a more appropriate response to the complaints made to it by the complainant.

Findings and declarations

The Commissioner found that AMEX interfered with the complainant's privacy within the meaning of s 13(1) of the Privacy Act by failing to take such steps as were reasonable in the circumstances to protect the complainant's personal information from unauthorised access, in breach of APP 11.1. The Commissioner made a number of declarations under s 52(1)(b) and s 52(3) of the Privacy Act, including that AMEX must:

- issue a written apology to the complainant, acknowledging its interference with the complainant's privacy;
- within 6 months of the date of the determination, implement account-level Access Logging and Action Logging across the Relevant Systems to the extent these are still in operation – to the effect that when an employee accesses or takes action on a customer's records, a time-stamp log entry is recorded;
- within 6 months of the date of the determination, implement technical controls across the Relevant Systems to enable AMEX to restrict its employees' access to specific customer information, including to protect the personal information of vulnerable or high-profile customers (for example, through individualised contact arrangements);
- pay the complainant specified amounts for economic loss, non-economic loss caused by the interference with the complainant's privacy and reimbursement of expenses the complainant incurred making the complaint.

Compliance with APP 1.2

In the course of the OAIC's investigation, it became apparent that AMEX's handling of the complaints made to it by the complainant raised questions about the AMEX's compliance with APP 1.2 during the Relevant Period. APP 1.2 requires APP entities to take such steps as are reasonable in the circumstances to implement practices, procedures and systems, relating to

the entity's functions or activities, that will enable them to comply with the APPs (APP 1.2(a)) and deal with complaints and enquiries about their APP compliance (APP 1.2(b)).

The complainant expressed concern that, following their complaint to AMEX, the employee retained the ability to access their account, and furthermore, that AMEX provided the complainant with incorrect information with respect to this issue. In investigating these allegations, the OAIC identified inaccuracies in the information that AMEX provided the complainant and others about the employee's ongoing access to the complainant's personal information. The evident deficiencies in the respondent's complaint-handling in this matter raised questions about the adequacy of the respondent's overall policies, procedures and systems for handling complaints about its APP compliance.

However, the OAIC's investigation was into a privacy complaint made to the OAIC by an individual complainant. Consequently – and for the reasons outlined below - potential breaches of APP 1.2 were not within the scope of the investigation or determination.

Section 36 of the Privacy Act permits an individual to complain about an act or practice that may be an 'interference with the privacy of [that] individual'. Such an interference occurs where the act or practice breaches an APP in relation to personal information about the individual (s 13(1)(a)). While the Privacy Act could be clearer with respect to this issue, it is unlikely that a breach of APP 1.2 constitutes an 'interference with the privacy of an individual'. An investigation under APP 1.2(b) would need to consider the steps an entity has taken to implement 'policies, procedures and systems' to ensure it can deal with complaints about its APP compliance. An investigation in this vein would extend beyond how an entity handles any one individual's personal information – rather, it would consider an entity's holistic approach in implementing systems to deal with privacy complaints.

Moreover, the Privacy Act does not confer a specific power to investigate possible breaches of APP 1 (including APP 1.2) in the context of a privacy complaint. By contrast, the Commissioner is explicitly empowered to investigate potential breaches of APP 1 in investigations commenced on her own initiative, pursuant to section 40(2)(a).

As such this investigation into the acts and practices of AMEX did not make findings with respect to APP 1.2 compliance. However, in the interest of promoting understanding and acceptance of the APPs, in her determination issued to AMEX the Commissioner drew AMEX's attention to APP 1.2 requirements with respect to implementing systems to deal with privacy complaints. In particular, the determination noted that where an entity receives a complaint relating to an employee accessing a complainant's personal information, the entity should have in place practice, procedures and systems to restrict that employee's access to that information, as a critical avenue to deal with the complaint.

Publication of determination and report

Section 52(5A) of the Act gives the Commissioner a discretion to publish the determination on the OAIC's website.

In deciding whether to exercise that discretion in this matter, the Commissioner gave consideration to a range of issues, including the nature of the issues that the determination

deals with, the prejudice to the parties, the implications for individual privacy, and the objects of the Act, The Commissioner decided not to publish the full determination in this matter on the OAIC website.

However, having regard to the matters listed in s 33B(2) of the Privacy Act, the Commissioner was of the view that publishing this report, which includes a detailed summary of the determination and the Commissioner's findings, would be in the public interest. Publishing details of the determination serves the public interest by highlighting to APP entities the need to take reasonable steps to protect personal information from insider security risk, and to put in place appropriate policies, procedures and systems for handling complaints about APP compliance, particularly when those complaints involve allegations against an entity's employees.