Security

WEB FRAUD AND FISHING

WWW.AURA.CO.TH

Web Fraud and Phishing

Protecting the Aura Name, Our Clients and Our Community

In an increasingly connected business environment, trust has become one of the most important assets of any institution. For a global investment, advisory and business group such as **Aura Solution Company Limited**, that trust extends beyond financial and commercial relationships. It encompasses the integrity of the Aura name, the confidence of our clients and counterparties, the security of our communications, and the protection of the individuals and organizations with whom we work.

Unfortunately, established corporate names can also become targets for fraud and impersonation. Individuals and organized groups may attempt to misuse the Aura name, corporate identity, websites, logos, documents, employee identities or other publicly available information in order to create the appearance of a legitimate relationship with Aura.

These activities may take many forms. They may involve fraudulent investment proposals, false employment opportunities, phishing emails, telephone scams, fake websites, impersonation of executives or employees,

fraudulent payment instructions, counterfeit documents, or unauthorized social-media and messaging accounts. In some circumstances, fraudsters may combine several of these methods, using an initial email or telephone call to establish contact before moving the conversation to another communication channel.

Such schemes can be sophisticated. They may use professional language, genuine photographs, copied corporate information and convincing documentation. A fraudulent communication may refer to real employees, genuine business activities or publicly available corporate information in an attempt to make the communication appear credible. In some cases, a fraudulent communication may appear almost indistinguishable from a legitimate business communication at first sight.

The existence of familiar information, professional presentation or corporate branding should therefore never be treated as sufficient evidence of authenticity. A genuine name can be used by a fraudulent person, a genuine document can be copied, and genuine corporate information can be reproduced without authorization.

For this reason, **verification should always take precedence over appearance**.

This article explains the principal forms of fraud and impersonation associated with corporate identity misuse and provides guidance for clients, business partners, candidates and members of the public who receive communications claiming to originate from Aura.

The Principle of Independent Verification

The most important safeguard against fraud is simple: **do not act on an important request until you have independently verified its source.**

Fraudsters frequently rely on urgency. A recipient may be told that an investment opportunity is available for only a limited period, that a payment must be completed immediately, that banking details have changed, or that confidential information is required without delay. The sender may suggest that failure to act immediately will result in the loss of an opportunity, the cancellation of a transaction or another adverse consequence.

The purpose of this pressure is often to prevent the recipient from taking the time to question the request or consult another person. By creating a sense of urgency, the fraudster attempts to move the recipient directly from receiving the communication to taking the requested action.

A legitimate business communication should not require a recipient to abandon reasonable verification procedures. Where a matter involves money, confidential information, account access or a significant business decision, the recipient should take sufficient time to establish who is communicating, whether the communication is genuine and whether the requested action is actually authorized.

Independent verification is particularly important because the contact information supplied by a fraudster may itself be

fraudulent. An email may direct the recipient to a false website, a telephone number may connect to the impersonator, or a messaging account may use the name and photograph of a genuine Aura employee. Simply confirming information through the same communication channel does not establish authenticity.

Verification should instead be conducted through information obtained independently from a trusted Aura source or from an established business relationship whose authenticity is already known.

When dealing with an unexpected or unusual communication, the appropriate approach is therefore to pause the interaction, examine the circumstances carefully and verify the request independently before proceeding. This is especially important when the communication involves investment opportunities, payment instructions, banking information, passwords, authentication codes, personal information, confidential documents or requests for secrecy.

Pause. Examine. Verify. Then act.

Official Aura Information

The principal source of official information concerning Aura is the Aura corporate website, www.aura.co.th. The website should be regarded as the primary point of reference when seeking information about Aura, its activities, corporate communications and other official matters.

For general corporate enquiries, Aura may be contacted through its official general email address, .

When checking whether a communication is genuine, clients, counterparties, candidates and other recipients should access the Aura website independently rather than following a link contained in an unexpected email, message or document. Similarly, a telephone number, email address or messaging account provided by the person contacting you should not, by itself, be treated as confirmation of authenticity.

A fraudulent party may deliberately provide contact information that appears legitimate but is controlled by the fraudster. This can include a website address resembling the official Aura domain, an email address using a similar name, a telephone number presented as belonging to an Aura representative or a messaging account using Aura's name and corporate identity.

The safest approach is therefore to obtain contact information independently from an official Aura source and use that information to verify the communication. Where a communication concerns a financial transaction, investment opportunity, payment instruction, confidential information or another material business matter, independent verification should be completed before any action is taken.

Why Corporate Impersonation Works

Modern fraud does not necessarily look fraudulent. Sophisticated impersonation schemes can be carefully prepared to resemble genuine corporate communications, and the individual behind the communication may have conducted substantial research before approaching the intended recipient.

A fraudster may first study publicly available information about Aura and the person or organization they intend to contact. Information obtained from corporate websites, business directories, professional profiles, press articles, public records, social-media platforms and other sources can provide sufficient background to construct a convincing story and make an unsolicited communication appear familiar.

The fraudster may know the name of a senior executive, the names and positions of employees, the company's business activities, the names of clients or counterparties, the locations of offices, the appearance of corporate documents, the organization's branding or the nature of an existing or proposed business relationship. They may use this information in an email, telephone call, WhatsApp message, investment proposal or other communication in order to create confidence.

In some cases, the fraudster may also reproduce genuine documents, corporate terminology, photographs, signatures, logos or other publicly available material. The resulting communication may therefore appear sufficiently detailed and professional to persuade a recipient that the sender must be genuine.

The important point is that **knowledge of genuine corporate information does not prove that the person contacting you is genuine**. Information about an organization or its employees may be publicly available and can be copied or misused by third parties. Identity and authorization must therefore be established independently, particularly when a communication involves money, confidential information or a significant business decision.

Investment and Financial Fraud

Investment fraud is among the most serious forms of corporate impersonation because it may involve substantial financial losses. A fraudster may claim to represent Aura or to have access to an Aura investment, private transaction, financing arrangement or exclusive financial opportunity.

The proposal may be presented through a formal-looking investment memorandum, presentation, term sheet, agreement, financial statement, certificate or website. Fraudsters may also use corporate logos, names of genuine employees or apparently authentic correspondence to create the impression that the opportunity has been authorized or approved by Aura.

An unsolicited proposal may be particularly concerning where it promises unusually attractive returns or suggests that the opportunity is available only to a small number of selected investors. The fraudster may attempt to create

exclusivity by claiming that the investment is confidential, that allocation is limited or that the recipient has been given special access.

Warning signs may include promises of guaranteed returns, unusually high yields, risk-free investment, immediate profits, exclusive access, confidential investment opportunities, guaranteed allocation, special treatment for selected clients or pressure to transfer funds quickly.

The appearance of professional documentation does not establish authenticity. Fraudsters can reproduce logos, signatures, corporate terminology, financial presentations and other visual elements with considerable accuracy. Documents should therefore not be relied upon as the sole basis for establishing that an investment opportunity is genuine.

Anyone receiving an unexpected investment proposal claiming to originate from Aura should independently verify the identity of the sender and the nature of the opportunity before providing personal, financial or confidential information or transferring funds. Verification should be conducted using independently obtained Aura contact information rather than the contact details supplied within the proposal itself.

Phishing Through Email and Messages

Phishing is one of the most common methods used to obtain sensitive information or persuade individuals to take an action that benefits a fraudster. A phishing communication may appear to come from an Aura employee, executive, adviser or another trusted organization and may be presented as an ordinary business request.

The message may ask the recipient to confirm an account, review a document, update information, complete a payment, verify an identity, download a file or respond to an urgent business matter. In some cases, the communication may contain a link leading to a fraudulent website designed to capture usernames, passwords, payment information or other confidential data. Attachments may also contain malicious software or fraudulent documents.

Particular care should therefore be taken with unexpected communications containing login requests, payment instructions, password-reset requests, unexpected documents, account-verification requests, links to unfamiliar websites, software or application downloads, or requests for confidential information.

Before clicking a link, examine the destination carefully and consider whether you were expecting the communication in the first place. If there is any uncertainty, access the relevant website independently rather than using the link provided in the message. Where the communication claims to originate from Aura, the official Aura website should be accessed directly through www.aura.co.th.

The same caution should be applied to attachments. A document that appears to be an invoice, contract,

investment proposal or other ordinary business record should not be opened simply because it carries corporate branding or appears professionally prepared. Unexpected files should be independently verified before they are opened or downloaded.

Telephone and Voice Fraud

Fraud is not limited to written communications. **Vishing**, or voice phishing, involves telephone calls in which a fraudster attempts to obtain information or induce a financial transaction by pretending to represent a trusted organization.

The caller may claim to be an Aura executive, an Aura employee, an adviser, a financial institution, a regulator, a government authority or another trusted organization. The caller may already know the recipient's name, company, position or other information and may use that knowledge to create an impression of familiarity.

The caller may then attempt to create pressure by claiming that immediate action is required, that a payment must be completed, that an account requires verification or that confidential information is necessary to resolve an urgent matter.

A telephone conversation should never be considered sufficient evidence of identity. If a caller requests confidential information, authentication codes, banking information or an immediate financial transaction, the

recipient should not rely solely on the caller's explanation or the telephone number displayed on the device.

Where necessary, the conversation should be ended and the relevant organization contacted independently using a trusted telephone number or other official contact information. This prevents the recipient from relying on contact information controlled by the person making the suspicious call.

Payment and Banking Fraud

Payment fraud often takes advantage of established business relationships and familiar corporate procedures. A fraudster may impersonate an executive, employee, supplier or business partner and claim that payment instructions have changed.

The request may appear to be a routine administrative update. The sender may explain that a bank account has been replaced, that a transaction should be redirected or that a payment must be made to a different beneficiary. Because such requests can resemble ordinary business correspondence, they can be particularly difficult to identify without proper verification.

However, a change in bank-account information can have significant consequences.

Any new or amended payment instruction should be independently verified before funds are transferred.

This is particularly important where a bank account has changed, the beneficiary name has changed, a new payment destination is introduced, the request is unusually urgent, the request comes from an unfamiliar address, the sender asks that normal verification procedures be bypassed or the communication requests secrecy.

Established payment procedures should not be abandoned simply because a request appears to come from a familiar person. Never treat an email containing revised payment details as sufficient confirmation of the change. Where appropriate, the new instructions should be confirmed through an established communication channel already known to the recipient.

Executive and Employee Impersonation

Another increasingly common form of fraud involves impersonating senior executives or employees. A fraudster may use the name, position, photograph or other publicly available information relating to a genuine Aura executive and then contact a client, counterparty, supplier or other business partner.

The impersonator may claim to be travelling, unavailable by telephone or involved in a confidential transaction. They may explain that normal procedures cannot be followed and then request that a payment be made, information be disclosed or an unusual action be taken.

The fact that a request appears to come from a senior person should not reduce the level of verification required. Seniority does not, by itself, establish that a communication is genuine or that the requested action has been authorized.

In fact, requests involving significant financial or confidential matters should receive **greater scrutiny**, regardless of the apparent seniority of the person making the request. If the request is unusual, unexpected or inconsistent with established procedures, the identity of the requester and the instruction itself should be independently confirmed before any action is taken.

Recruitment and Employment Fraud

Corporate identity can also be misused to create fraudulent employment opportunities. An individual may receive an apparently genuine offer to work for Aura or an invitation to participate in a recruitment process. The fraudster may use Aura's name, corporate branding, employee information or apparently genuine employment documents to make the opportunity appear legitimate.

After establishing contact, the fraudster may request money for recruitment, administration, training, equipment, visas or other purposes. They may also request identity documents, banking information or other personal information through an unofficial website, email address or messaging account.

Aura does not require candidates to pay a fee in order to apply for employment.

Candidates should independently verify employment opportunities through official Aura channels before providing personal information, signing documents or making any payment. An unsolicited employment offer should be treated with particular caution where it involves financial requests, unusual recruitment procedures or communication through unofficial channels.

The use of Aura's name or corporate identity in a recruitment advertisement does not establish that the position or recruiter is genuine. Candidates should verify the opportunity independently before proceeding with the recruitment process.

Fake Websites and Domains

A fraudulent website can be one of the most convincing elements of an impersonation scheme because it may be designed specifically to create the appearance of a genuine Aura website. Fraudsters can reproduce corporate colours, logos, photographs, language, page layouts and other publicly available information to create a website that appears professional and credible. In some cases, the fraudulent website may contain substantial amounts of copied corporate information, making it difficult to distinguish from a legitimate website based on appearance alone.

The difference may exist only in the domain name or website address. A fraudulent website may use a domain that is visually similar to the official Aura address but contains additional words, unusual characters, spelling variations, different domain extensions, hyphens or other alterations. These differences can be easy to overlook, particularly when a website is accessed through a link contained in an email, message or other unsolicited communication.

The official Aura website is:

www.aura.co.th

Clients, visitors and other parties communicating with Aura should therefore pay close attention to the complete website address before entering information, downloading documents, submitting forms or taking any other action. A website should not be considered genuine simply because it displays the Aura name or uses Aura's corporate identity.

Particular caution should be exercised with website addresses containing additional words, unusual characters, spelling variations, different domain extensions, hyphens or additional symbols, as well as domains that merely resemble the official Aura address. Fraudsters may intentionally select addresses that are visually similar to legitimate domains in order to make them difficult to distinguish at a glance.

Where a website has been reached through an unexpected email, text message, WhatsApp communication or other unsolicited contact, users should avoid relying on the link

provided in that communication. When in doubt, type the official Aura website address directly into the browser or access it through an independently verified source. This reduces the risk of being redirected to a fraudulent website designed to collect personal, financial or confidential information.

The same principle applies to websites requesting payments, investment information, account credentials, identification documents or other sensitive information. Before providing such information, the identity and authenticity of the website should be independently established.

Social Media and Online Impersonation

Social-media platforms can provide fraudsters with another means of creating a false association with Aura. A fraudulent account may use the Aura name, corporate logo, employee photographs, descriptions of Aura's activities or other information copied from legitimate sources. The account may then be used to contact individuals directly and present investment proposals, recruitment opportunities, business opportunities or other requests that appear to originate from Aura.

The use of genuine corporate information does not establish that a social-media account is authorized. Fraudsters may copy information directly from legitimate websites or public profiles and use it to make an impersonation appear credible. Similarly, the use of the name or photograph of a

genuine Aura employee does not establish that the account is operated by that individual or that the person has authority to communicate on behalf of Aura.

Aura does not operate official corporate accounts on conventional social-media platforms such as Facebook, X, LinkedIn or Instagram. Accordingly, a social-media account using the Aura name, logo or employee information should not automatically be regarded as an official Aura channel.

Particular caution should be exercised when a social-media account contacts an individual unexpectedly, particularly where the communication involves an investment proposal, employment opportunity, business transaction, request for confidential information or request to transfer funds. Individuals should also be cautious where the sender attempts to move the conversation from an established business channel to a private messaging account or asks that normal verification procedures be bypassed.

Where a social-media account claims to represent Aura or one of its employees, its identity should be independently verified before any sensitive information is provided or any financial or business action is taken. The presence of corporate branding, photographs or apparently genuine information should not be treated as sufficient evidence of authorization.

WhatsApp Communications

Aura may use WhatsApp for appropriate communications with selected clients where a direct and efficient channel is required. WhatsApp can provide a practical means of

maintaining communication with established clients, particularly where timely and direct contact is appropriate.

However, the use of the Aura name, logo, employee name or corporate information by a WhatsApp account does not, by itself, establish that the account is genuine. As with other digital communication channels, information displayed on a profile can be copied or reproduced by individuals seeking to impersonate Aura or its personnel.

Where applicable, clients should look for the **official WhatsApp verification badge** associated with Aura's authorized account. The verification badge can provide an important indication that the account has been formally recognized by the platform. Clients should nevertheless consider the verification status together with the nature of the communication, the identity of the person involved and the request being made.

Particular care should be taken where a WhatsApp communication involves a significant financial transaction, a change to established payment instructions, a request for confidential information, account credentials, identification documents or another material business matter. In such circumstances, clients should independently confirm the communication through an established Aura contact channel before taking action.

The existence of a verified communication channel should not be interpreted as a reason to abandon normal security procedures. Clients should continue to exercise appropriate care when dealing with requests involving financial

information, payments, confidential information or other sensitive matters.

Where a WhatsApp communication appears unusual, unexpected or inconsistent with the established nature of the relationship, the safest approach is to pause the interaction and verify the matter independently using trusted Aura contact information.

Aura may use WhatsApp for appropriate communications with selected clients where a direct and efficient channel is required. WhatsApp can provide a practical means of maintaining communication with established clients, particularly where timely and direct contact is appropriate.

Aura's authorized WhatsApp communications are conducted through the following verified numbers:

+66 8241 88 111
+66 8042 12345

Clients should verify that communications claiming to originate from Aura are received through these authorized WhatsApp numbers and that the relevant WhatsApp account displays the **official verification badge**. The presence of the Aura name, logo, employee name or corporate information on a WhatsApp profile should not, by itself, be regarded as evidence that the account is genuine, as such information can be copied or reproduced by third parties seeking to impersonate Aura.

The verification badge provides an additional means of distinguishing an authorized Aura WhatsApp presence from

an account that merely uses the Aura name or corporate identity. Clients should nevertheless consider the verification status together with the nature of the communication, the identity of the person involved and the request being made.

Particular care should be taken where a WhatsApp communication involves a significant financial transaction, a change to established payment instructions, a request for confidential information, account credentials, identification documents or another material business matter. In such circumstances, clients should independently confirm the communication through an established Aura contact channel before taking action.

A verified WhatsApp account should not be interpreted as a reason to abandon normal security procedures. Clients should continue to exercise appropriate care when dealing with requests involving financial information, payments, confidential information or other sensitive matters.

If a person claiming to represent Aura contacts you through a WhatsApp number other than the authorized numbers identified above, particularly where the communication involves money, investment opportunities, confidential information or urgent action, the communication should be treated with caution and independently verified before any action is taken.

Recognizing the Warning Signs

Fraudulent communications often contain several indicators that may help identify them before any harm occurs. These indicators can appear in emails, telephone calls, WhatsApp messages, websites, documents, social-media communications or other forms of contact. While any individual warning sign may have an innocent explanation, several unusual characteristics appearing together should be treated as a reason to stop and verify the communication before taking further action.

Unusual Urgency

You are told that immediate action is required and that there is no time for verification. The sender may create pressure by suggesting that a payment, investment, business opportunity or other matter must be completed immediately. Unusual pressure should be treated carefully, particularly where the request involves money, confidential information or account access.

Financial Pressure

You are asked to transfer funds immediately or to a new or unfamiliar account. The request may be presented as a payment instruction, investment requirement, transaction, fee or other business matter. Any unexpected request involving the transfer of funds, particularly where banking

details have changed, should be independently verified before payment is made.

Requests for Secrecy

You are asked not to discuss the request with colleagues, advisers, banks or other representatives. Fraudsters may use secrecy to prevent the recipient from independently checking the identity of the sender or the legitimacy of the request. A request for confidentiality should therefore be considered carefully when it is combined with unusual urgency, financial instructions or requests for sensitive information.

Unusual Contact Details

The email address, telephone number, website or messaging account does not correspond with information obtained independently. Fraudsters may use contact details that closely resemble legitimate Aura information while making small changes to names, domains, telephone numbers or other identifying details. The name displayed on an account should not, by itself, be considered proof that the account belongs to the person or organization it claims to represent.

Suspicious Links

A link appears familiar but directs you to an unexpected or unfamiliar website. Fraudulent links may be designed to resemble legitimate websites while directing users to a different destination. Particular caution should be exercised where a link requests personal information, banking details,

passwords, authentication codes or other confidential information.

Unexpected Attachments

You receive a document or file that you were not expecting. Unexpected attachments may appear to be invoices, contracts, investment documents, recruitment material or other legitimate business records. Do not open or download an unexpected attachment until its source and purpose have been independently verified.

Requests for Security Credentials

You are asked for a password, authentication code, security token or other confidential credential. Such information should not be provided in response to an unsolicited request, even if the person making the request claims to be an Aura employee, executive, adviser or other trusted representative.

Aura will not ask you to disclose your password or authentication code through an unsolicited communication.

Unsolicited Investment Opportunities

You are approached unexpectedly with an investment proposal claiming to be associated with Aura. The communication may include investment documents, financial information, corporate branding or other material intended to make the opportunity appear genuine. Particular caution should be exercised where an unsolicited proposal

involves unusually attractive returns, immediate action, requests for confidentiality or instructions to transfer funds.

Unofficial Recruitment

You are offered employment through an unverified platform or asked to pay money as part of the recruitment process. Fraudulent recruitment communications may use the Aura name, corporate identity or employee information to create the appearance of a genuine employment opportunity. Candidates should independently verify recruitment communications before providing personal information or making any payment.

None of these indicators necessarily proves that a communication is fraudulent. However, several warning signs occurring together should be treated as a reason to stop and verify the communication independently.

Protecting Your Information

Good security practices remain one of the most effective defenses against fraud. Personal, financial and confidential information should only be provided when the identity of the recipient and the purpose of the request have been properly established.

Never disclose passwords, authentication codes, security tokens or similar credentials in response to an unsolicited request.

Aura will not ask you to disclose your password or authentication code through an unsolicited communication.

Do not install software, applications or browser extensions supplied through unexpected messages. Such files may be presented as legitimate business, security, investment or recruitment applications but may expose information or provide unauthorized access to a device or account.

Do not open suspicious attachments, particularly where the document was not expected or the sender cannot be independently confirmed.

Do not enter confidential information into a website simply because the website looks professional. Fraudulent websites may reproduce corporate logos, photographs, colours, documents and other visual elements to create the appearance of legitimacy.

And do not assume that a person is genuine simply because they know information about you or your organization. Fraudsters may obtain names, job titles, company information and other details from publicly available sources or other compromised information and use them to make an impersonation appear credible.

If You Suspect Fraud

Receiving a communication that may be fraudulent can be concerning, particularly when the sender appears to represent a trusted institution, executive, employee, adviser

or business partner. Fraudulent communications are often designed to appear credible and may use familiar names, corporate branding, professional language and apparently genuine documents to create a false sense of legitimacy. The most important response is therefore to remain calm and avoid taking further action until the communication has been independently verified.

If you receive an email, telephone call, WhatsApp message, document, website link or other communication that you believe may be fraudulent, stop before responding or taking any action. Do not continue the conversation simply to determine whether the individual is genuine, and do not allow the person contacting you to control the verification process by providing alternative contact details or directing you to another website. In particular, do not click links, open unexpected attachments, download files, disclose passwords or authentication codes, provide banking or confidential information, or transfer funds based solely on the communication.

Instead, preserve the communication and begin an independent verification process. This is particularly important where the communication involves money, investment opportunities, payment instructions, personal information, account credentials or other confidential matters.

Preserving Evidence

If you suspect that you have encountered fraud, retain the original communication wherever possible. Do not

immediately delete emails, messages, documents or other material simply because they appear suspicious. Such information may later assist Aura, a financial institution, a technology platform or the relevant authorities in understanding what occurred and identifying the source of the activity.

Useful evidence may include the original email and complete sender information, telephone numbers, WhatsApp or other messaging records, website addresses, screenshots, documents, contracts, investment proposals, invoices, payment instructions, bank-account details, transaction references, names used by the individual, and the dates and times of communications.

Where possible, preserve the material in its original form. Avoid altering or deleting information that may help establish how the communication was received and what was requested.

Independent Verification

Once you have stopped the communication and preserved the relevant information, the next step is independent verification. Do not use the telephone number, email address, website or messaging account provided by the suspected fraudster to verify their identity. Doing so may simply return you to another channel controlled by the same individual.

Instead, obtain contact information independently from an official Aura source or from an established business relationship that you already know to be genuine.

The official Aura website is www.aura.co.th and the general corporate email address is .

If the communication claims to come from a particular Aura employee, executive or representative, independently confirm the person's identity through a trusted channel rather than replying to the original message or using the contact details contained within it.

Independent verification is particularly important because sophisticated fraudsters may know the names, positions and responsibilities of genuine Aura personnel and may use that information to make an impersonation appear authentic.

If You Have Already Transferred Funds

If you have already transferred money as a result of a communication that you now believe may be fraudulent, contact your bank or relevant financial institution immediately. Do not wait until you have established with certainty that fraud has occurred. Where a payment may have been made as a result of deception, prompt notification allows the financial institution to assess the circumstances and determine what measures may be available.

When contacting your bank, provide as much information as possible about the transaction. This should include the date and time of the payment, the amount and currency, the recipient's name and account details, the receiving bank, the transaction reference, any invoice or payment instruction you received, and the communications that led to the transfer.

Retain copies of all relevant correspondence and documentation and provide them to the financial institution when requested. If the transaction involved a payment platform, card provider or other financial service, that organization should also be contacted promptly.

Do not assume that nothing can be done simply because a payment has already been processed. The appropriate response is to report the matter immediately and allow the relevant institution to assess the transaction.

Where appropriate, the incident may also be reported to the relevant platform or competent authority in the jurisdiction concerned.

If You Have Disclosed Personal or Confidential Information

Fraud does not always begin with a request for money. In many cases, the initial objective is to obtain information that

can later be used for unauthorized access, identity fraud, further impersonation or financial crime.

Information disclosed to a fraudster may include passwords, authentication codes, banking information, identification documents, personal details, corporate information or other confidential material.

If you have disclosed sensitive information, take appropriate steps to secure the affected account, system or service as soon as possible. Depending on the nature of the information disclosed, this may include changing passwords, resetting authentication credentials, strengthening account security, contacting your bank or financial institution, notifying the relevant service provider and monitoring accounts for unusual activity.

If corporate or confidential business information has been disclosed, the relevant organization should also be informed so that appropriate protective measures can be considered.

Most importantly, do not provide additional information to the individual who originally requested it. A fraudster may attempt to contact the same person again using a different identity or explanation, particularly if they believe that the first interaction was successful.

Reporting Fraudulent Use of the Aura Name

The unauthorized use of the Aura name, corporate identity or employee identities should be treated seriously. Fraudulent activity may involve websites, email addresses, WhatsApp accounts, social-media profiles, investment platforms, recruitment advertisements, documents or other communications that falsely suggest an association with Aura.

Where appropriate, suspicious activity may be reported directly to the relevant platform or service provider. A fraudulent social-media or messaging account can generally be reported through the platform on which it operates, while suspicious financial activity should be reported to the relevant bank or financial institution. Depending on the circumstances and jurisdiction, suspected fraud or cybercrime may also be reported to the appropriate authorities.

If you believe that a communication falsely represents itself as originating from Aura, you may contact Aura using independently verified official information.

Aura Solution Company Limited

Official Website: www.aura.co.th

General Enquiries:

When contacting Aura about suspected fraud, do not use contact information supplied by the suspected fraudster. Obtain the relevant contact details independently from the official Aura website or from an established and trusted business relationship.

Where appropriate, provide the relevant evidence, including copies of suspicious communications, website addresses, account information, documents and other material that may assist in identifying the activity.

Protecting Trust

The protection of a corporate identity is ultimately about protecting trust. Aura's name represents relationships built over time with clients, counterparties, employees, advisers and other stakeholders. The unauthorized use of that identity can create confusion and may expose individuals and organizations to financial, operational and personal risk.

For this reason, anyone who encounters a communication bearing the Aura name should consider not only whether the communication looks genuine, but whether its source and purpose have been independently established. Professional presentation, familiar branding or knowledge of genuine corporate information should never replace proper verification.

A convincing document can be copied. A corporate logo can be reproduced. An employee's name and photograph can be misused. A website can be designed to resemble a legitimate corporate website. What establishes authenticity is not appearance, but independent verification.

A Simple Principle

When a person claims to represent Aura, consider who is contacting you, how their identity can be independently established, whether the website or communication channel is genuinely associated with Aura, whether the request is consistent with the nature of the relationship, and whether the instruction has been independently verified before any action is taken.

If there is uncertainty at any stage, the appropriate course is to pause and verify the matter before proceeding. There is rarely a good reason to allow an unexpected request involving money, confidential information or account access to dictate the speed at which you respond.

For official corporate information, always begin with Aura's official website and use independently verified contact information.

Aura Solution Company Limited
www.aura.co.th