

# BITS

---

FINANCIAL SERVICES  
R O U N D T A B L E

## **BITS KEY CONSIDERATIONS FOR GLOBAL BACKGROUND SCREENING PRACTICES**

**JUNE, 2005**

**Disclaimer**

THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. Neither the individual member companies nor BITS and The Financial Services Roundtable make any warranty or assume any legal liability or responsibility for the accuracy, completeness or usefulness of the information contained in this document, or represent that this document's use would not infringe privately-owned rights. Reference to any special commercial products, processes or services by trade name, trademark, service mark, manufacturer or otherwise does not necessarily constitute or imply its endorsement, recommendation or favoring by BITS or The Financial Services Roundtable.

## TABLE OF CONTENTS

I. Overview	4
II. Regulatory and Legal Requirements for Background Checks	6
III. Risk and Mitigating Factors: Considerations for Background Screening Requirements	10
IV. Background Screening Criteria: Country Issues	14
Appendix I: Country Matrices	
Asia Pacific	16
Europe	21
North and South America	22
Africa and Middle East	23
Appendix II: About the Authors	24

## **BITS KEY CONSIDERATIONS FOR GLOBAL BACKGROUND SCREENING PRACTICES**

### **I. OVERVIEW**

According to the August 2004 U.S. Secret Service and CERT<sup>®</sup> Coordination Center's *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*:

... (The fact that) over one quarter of the insiders had a criminal record prior to their incidents underscores the importance of looking into employee backgrounds prior to hiring. Background checks for prospective, and current, employees that include at least basic criminal history checks may help identify employees with histories of fraud, theft, or other criminal behavior.<sup>1</sup>

Effective financial institution due diligence and outsourcing management programs should evaluate the partner company's financial statements and controls for technology, processes and procedures, including the employees and principals involved in the outsourced relationship.<sup>2</sup> As part of that evaluation, and consistent with the institution's internal policies and procedures, financial institutions should understand their global sourcing partners' employment, hiring, training, and firing policies and criteria.

When outsourcing domestically, organizations generally understand what background check information is available, what type of information can be requested and when, and the acceptable processes and approvals required for conducting checks. However, for global operations and sourcing, financial institutions need to be familiar with local employment guidelines and laws that may impact the availability and reliability of employee background information as well as any related legal or humanitarian issues.

In many global sourcing arrangements, the service provider performs all of the functions related to employee hiring. Often, the service provider's management knows the country-specific practices and requirements, helping to ensure that the financial institution does not trigger any employment issues. Regardless of why the service provider performs the hiring functions, in these situations financial institutions should identify and manage the risks using controls such as specifying background screening requirements in the service provider contract, identifying requirements for the background check and auditing hiring practices to ensure requirements are being met.

This document, *BITS Key Considerations for Global Background Screening Practices*, was developed to provide BITS members with information on risk and mitigation strategies related to global outsourcing of functions related to financial services. There are three primary sections:

- Overview of the financial industry's legal and regulatory requirements;

---

<sup>1</sup> U.S. Secret Service and CERT Coordination Center/SEI, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, August 2004.

<sup>2</sup> See the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*, November 2003, for further details on selecting and managing service provider relationships.

- Strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and
- Information which is available by country to validate identity and background.

Each section explains financial institutions' most important considerations for global employee screening policies, programs and requirements.

Financial institutions should selectively apply the guidelines in this *BITS Key Considerations for Global Background Screening Practices*, based on the institutions' risk-assessment results and the type of outsourcing engagement. The document should be used as a reference, stimulating firms to ask the right questions and complementing individual institutions' risk-management policies.

It is important to recognize that **country risk is dynamic**. As a result, this may impact the availability, accuracy and timeliness of employee information as well as change the risk profile of the country to which functions are being outsourced. When utilizing the *BITS Key Considerations for Global Background Screening Practices*, it is important to note that the matrices of available information by country were developed as of a point in time.

Further, the information in this document should be used in conjunction with a financial institution's country risk analysis. An understanding of the political and economic environment will be helpful in assessing the reliability and accuracy of information available about individuals being considered for employment. Further guidelines for assessing country risk can be found in Section 9.3 of the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*.

It should also be noted that **international privacy laws are complex**. *The BITS Key Considerations for Global Background Screening Practices* does not address any of the complex issues related to a financial institution's ability to access and/or transmit information. For example, accessing employee information in some countries depends on the relevance of the information to the job position and responsibilities. Further, privacy laws are a factor in determining whether information may be transmitted to other countries.

The *BITS Key Considerations for Global Background Screening Practices* was developed by a small, dedicated team of professionals from the BITS IT Service Provider Working Group and BITS staff. Two global background screening companies, Kroll Worldwide and First Advantage-Quest Research, provided valuable contributions to the document. For further information, please contact Faith Boettger, BITS Senior Consultant, at [Faith@fsround.org](mailto:Faith@fsround.org) or [John](mailto:John@fsround.org) Carlson, Senior Director, at [John@fsround.org](mailto:John@fsround.org).

## II. REGULATORY AND LEGAL REQUIREMENTS FOR BACKGROUND CHECKS

The following is a partial listing of regulatory and legal requirements that apply to US financial institutions. It is not intended to be a comprehensive listing of all such laws and regulations, but rather outlines those that were included in the analysis performed by the Working Group. This document does not consider data privacy implications related to the transfer of information outside of certain countries or the requirements imposed on global financial institutions operating in other countries.

<i>Agency</i>	<i>Guidance #</i>	<i>Date</i>	<i>Title</i>	<i>Background Check Reference</i>
FFIEC		June 2004	IT Outsourcing Technology Handbook	Due Diligence section (pg. 11) - Qualifications, backgrounds, and reputations of company principals including criminal background checks where appropriate.
FFIEC		12/2002	FFIEC IT Examination: Handbook: Information Security	<p><b>BACKGROUND CHECKS AND SCREENING</b></p> <p>Financial institutions should verify job application information on all new employees.</p> <p>The sensitivity of a particular job or access level may warrant additional criminal background and credit checks. Institutions should verify that contractors are subject to similar screening procedures. Typically, the minimum verification considerations include</p> <ul style="list-style-type: none"> <li>• Character references;</li> <li>• Confirmation of prior experience, academic record, and professional qualifications; and</li> <li>• Confirmation of identity from government issued identification.</li> </ul> <p>After employment, managers should remain alert to changes in employees' personal circumstances that could increase incentives for system misuse or fraud.</p>
FFIEC		11/28/2000	Risk Management of Outsourced Technology Services	Operations and Controls: Determine adequacy of the service provider's standards, policies and procedures relating ... and employee background checks.

<i>Agency</i>	<i>Guidance #</i>	<i>Date</i>	<i>Title</i>	<i>Background Check Reference</i>
FFIEC	501B exam practices/ OCC 2001-35 Attachment A		Examination procedures to evaluate compliance with the guidelines to safeguard customer information	Dual Control Procedures, segregation of duties, and employee background checks. Check standard internal control procedures to minimize fraud and other risks. In general, only employees should have access to customer information or customer information systems necessary to perform job functions.
FFIEC		Apr-01	Privacy of Consumers' financial information Part 12 501(b) and Bank Management	Operational policies (such as dual control procedures, segregation of duties, and employee background checks).
OCC AL	2001-04		Identity Theft and Pretext Calling	Because insiders may be identity thieves a bank should consider conducting background checks for its employees. Where indicated by its risk assessment, a bank should also monitor its service providers to confirm that they have implemented appropriate measures to limit access to customer records.
OCC AL	2001-2		Privacy Preparedness	Banks should determine whether their agreements with nonaffiliated third parties that involve the disclosure of nonpublic personal information meet the regulatory requirements for maintaining the confidentiality of the bank's consumer information.
OCC AL	2001-9		Third Party Risk	Due Diligence in Selecting a Vendor - qualifications, backgrounds, and reputations of company principals.
OCC	2000-25		Privacy Laws and Regulations	
OCC	2002-16	5/15/2002	Bank Use of Foreign-Based Third-Party Service Providers	The relationship must not inhibit a bank's ability to comply with all applicable US laws and regulations.
OCC	2001-47	11/1/2001	Third Party Relationships: Risk Management Principles	Banks should also consider how best to ensure that third parties meet information security and customer privacy requirements. A bank's due diligence should include the qualifications, backgrounds, and reputations of company principals, to include criminal background checks, when appropriate. The third party must implement appropriate security measures designed to meet the objectives of regulatory guidelines with which the bank must comply. The bank must monitor controls such as reviewing the third party's policies relating to internal controls and security to ensure that they continue to meet the bank's minimum guidelines and contract requirements.
OCC AL	2000-12	11/28/2000	Risk Management of Outsourcing Technology	No mention of background checks

<i>Agency</i>	<i>Guidance #</i>	<i>Date</i>	<i>Title</i>	<i>Background Check Reference</i>
OCC	2001-8	7/30/2001	Authentication in an Electronic Banking Environment	No mention of background checks
OCC	12 CFR Part 40	6/1/2000		No mention of background checks
OCC	12 CFR Part 30 Appendix B	7/1/2001	Interagency Guidelines Establishing Standards for Safeguarding Customer Information	Manage and Control Risk. Each bank shall have: Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information.
FDIC	Section 19 of 12 U.S.C 1829	Dec-98	FDIC Statement on Policy for Section 19 of the FDI Act	Section 19 imposes a duty upon the insured institution to make a reasonable inquiry regarding an applicant's history, which consists of taking steps appropriate under the circumstances, consistent with applicable law, to avoid hiring or permitting participation in its affairs by a person who has a conviction or program entry for a covered offense.
OTS	TB-82a	September 2004	Third Party Arrangements	Internal control environment: the association should determine the third party's standards, policies, and procedures related to internal control, maintenance records, privacy protection, facilities management, security, contingency plans, and employee background checks.
SEC	Release No. 34-50157; File No. SR-NASD-2004-095	August 5, 2004	Self-Regulatory Organizations; Notice of Filing and Immediate Effectiveness of Proposed Rule Change by National Association of Securities Dealers, Inc. Adopting a Fingerprinting Program for NASD Employees and Independent Contractors in the State of New York, and, as Dictated by Business Need, in Other Jurisdictions	Pursuant to New York State law, the NASD proposes to adopt a program for conducting fingerprint-based background checks of NASD employees and independent contractors in the State of New York, and in other jurisdictions as business need may dictate.

<i>Agency</i>	<i>Guidance #</i>	<i>Date</i>	<i>Title</i>	<i>Background Check Reference</i>
NRIC	6-6-5033		NRIC Best Practices	Service Providers, Network Operators and Equipment Suppliers should consider establishing and implementing background investigation policies that include criminal background checks of employees, contractors, and vendors. The policy should include disqualification criteria. Audit to ensure compliance.
NRIC	6-6-8099		NRIC Best Practices	Create policy on personnel hiring merits: Service Providers, Network operators and Equipment Suppliers should perform background checks consistent with the sensitivity of the staff member's responsibilities to verify employment history, education, and certification.

### III. RISK AND MITIGATING FACTORS: CONSIDERATIONS FOR BACKGROUND SCREENING

#### Requirements

When financial institutions create background screening requirements, they must identify strategies that protect and mitigate risk based on the unique nature of the outsourced engagement. Institutions should consider these specific areas of control:

- **Data Considerations:** Does the outsourced application, system or service allow access to sensitive information?
- **Technical Controls:** What controls are in place to prevent and detect access to systems by both authorized and unauthorized users?
- **Logical Controls:** What network service provider controls are in place? When in the process are employees allowed systems access?
- **Physical Controls:** What controls are in place at the service provider to restrict access to facilities, documentation, systems, etc.?

Once the financial institution has reviewed the risk environment and identified regulatory and corporate requirements, it should consider whether or not the organization can define one or many tiers of background screening requirements. These definitions should be based on the:

- Controls outlined above;
- Country risk analysis including hiring and termination requirements by country;
- Level of systems access required to perform employee responsibilities ; and
- Availability of information as outlined in the country matrices attached.

An example of tiering might include requirements such as the following:

Level of Risk	Background Screening Requirements
Low Risk	Name Social Security Number/ID Number Address Verification of Educational Background Previous Employment
Medium Risk	Low Risk Requirements Credit Check Criminal Background Check
High Risk	Medium Risk Requirements Interpol Search Polygraph Drug Screening

### Examples of Mitigating Factors for Deficiencies in Offshore Background Investigations

The following provides a high level overview of some of the controls which should be evaluated. For a more detailed review of controls, please refer to the *BITS Framework for Managing Technology Risk for Information Technology (IT) Service Provider Relationships and Expectations Matrix*.

<b>Company Level</b>	<b>While a full due diligence on the company includes a review of financials, controls, management, strategy, etc. when evaluating requirements for background checks on employees, there are several areas that warrant attention.</b>
Classification of Company	The reputation and maturity of a given corporation are often good indicators of the effectiveness of its hiring practices and employee vetting process. Factors such as industry certifications (e.g., CMM, ISO 17799), years of experience, stock performance, staff retention and client list (e.g., Is there a financial industry focus?) should all be considered.
HR Policies and Procedures	Well documented and consistently applied HR policies can reduce the risk of hiring individuals that would place the service provider and its clients at risk.
Auditing Employment Records	Review records for evidence that policies are consistently applied to hiring and employment decisions.
Security Policies, Procedures and Training	Well documented and consistently applied security policies, procedures and training increase the likelihood that the provider would detect and address malicious behavior. <sup>3</sup>
Reputation	Given the level of competition for offshore business, a company's reputation could be irrevocably marred if a major security breach were perpetrated by one of its employees. The <i>expectation</i> is that management within these corporations would demand that employees be thoroughly vetted prior to placing them in a situation where their actions could be particularly damaging to a client.
Insurance	Requirement of bond insurance is one effective incentive to properly screen applicants using the best possible means within their country's infrastructure and legal system. The validity of this insurance and the requirements for foreign entities to collect on it should be clearly documented and verified using offshore legal counsel.
Contract	Contract language should address financial institution regulatory requirements and financial penalties for security breaches committed by service provider staff. Just as with bond insurance, however, the ability of the client organization to actually enforce and collect on contract terms of this nature should be researched by experts on the legal system of the country in question. Resources such as local counsel or the US Embassy Regional Security Officer located in the country may also provide relevant insight.
<b>Data Characteristics</b>	<b>Careful assessment of the type of data access that will be granted to a given service provider may dictate the level of emphasis that should be placed on the background investigation practices. Careful consideration should be given to the possibility of the data content or quantity changing later in the relationship. If this is</b>

<sup>3</sup> Additional information on security awareness and training can be found in "BITS Critical Success Factors for Security Awareness and Training Programs," June 2005.

	<b>possible, the higher standard should be applied from the start of the relationship.</b>
Content	The content of information processed by the service provider should be considered when determining the adequacy of the scope of background investigations performed by the service provider (e.g., non-public personal information).
Quantity	The quantity of (sensitive) information accessible by a given contractor over a specified period of time is also a factor to consider. For example, a telemarketing agent generally has access to much less information than a database support specialist for back end customer service systems.
<b>Technical Controls <sup>4</sup></b>	
	<b>These controls indicate the misuse—or attempted misuse—of granted access levels by third parties. In some cases technical controls can prevent this misuse. Technical controls consist of two general types:</b> <ul style="list-style-type: none"> <li>• <b>Those that detect attempts to elevate privileges in order to access information that is not permitted.</b></li> <li>• <b>Those that would detect misuse of granted access levels.</b></li> </ul>
Firewalls	Firewalls can indicate when users are attempting to exploit granted access to gain unauthorized access, and potentially prevent the same.
Intrusion Detection	Intrusion detection can indicate when users are attempting to exploit granted access to gain unauthorized access, and potentially prevent the same.
Log Analyzers	Application and system logs can be indicators of individuals attempting to elevate privileges or to execute commands that are not authorized.
Link Encryption	Encryption, particularly when implemented from the desktop to the far end, virtually eliminates the possibility of anyone “sniffing” traffic as it traverses the vendor’s network.
Segregation of Duties	Verify and segregate key duties (e.g., individuals who authorize access, personnel who enable access, and personnel who verify access).
Technical Standards	A company should use a standard desktop configuration to define the baseline desktop settings and system requirements, control acceptable devices (e.g., wireless) and access (e.g., Internet). Audits used to ensure that unapproved software and devices are not in use.
<b>Physical Controls</b>	
	<b>These controls are implemented at the service provider location to ensure that individuals are compelled not to remove information from a given area.</b>
Facility	Consideration should be given to whether the facility is shared or dedicated. If the facility is shared, the risk assessment may need to include a review of the tenants of the building and the nature of their business, as well as the physical location of the operations within the building (e.g., Is the facility on ground, below ground, or at roof level? Are there windows in the facility?).

<sup>4</sup> To the extent that technical controls over system access are at issue, it is important to recognize that monitoring of employees’ electronic communications and activities is subject to complex state and federal privacy and wiretapping regimes embedded with serious penalties for violation. Source: Foley Hoag

Cameras	Depending on the placement, cameras deter individuals from attempting to record data and/or remove it from a secured area.
Guards	Guards provide further enforcement of policies restricting who/what enters and leaves a secured area.
Paperless Work Environment	When feasible (and properly implemented and enforced), establish an effective means to prevent significant amounts of paper media from leaving a secure environment and the recording of confidential information on such.
Disable Input and Output Ports/Devices	Disabling floppy drives, CD-RWs, and USB, parallel and serial ports on systems being utilized significantly reduces the potential for extrication of information from the environment.
Secure Disposal of Paper and Electronic Media.	Organizations should have procedures and controls for disposal and reuse of equipment and software, especially for those with sensitive customer information.

#### IV. BACKGROUND SCREENING CRITERIA: COUNTRY ISSUES

The main components of financial institution background screenings are:

- Identity;
- Educational and professional qualifications;
- Employment history;
- Criminal records;
- Credit history; and
- Public records searches.

When developing background screening requirements, financial institutions should understand relevant laws (e.g., privacy and employment laws), the accuracy of the information obtained, and the time it will take to obtain the information. For each country named in Appendix II, the information availability matrix indicates whether certain information is available but does not, in all cases, provide details on the reliability or accuracy of the information provided. Again, it is important to note that the availability of this information is provided as of a point in time and may change, given the dynamic nature of country environments.

- **Country Analysis.** The information contained in the matrices provides an overview of the information that is available by country but does not provide insights into the reliability or accuracy of recordkeeping practices, corruption rates, or legal considerations relative to the information. As stated previously, country risk is dynamic and should be monitored for changes which may impact these issues.
- **Employment Issues.** When developing a background screening process, financial institutions should also understand employment laws which might impact hiring, screening and termination requirements. The risks associated with each may drive the level of checks.
- **Past Employment.** Employees may have work experience in countries outside of where they are currently domiciled or country of passport. For example, an employee working at the financial institution's US operations may establish a credit or criminal record that should be reviewed.
- **Use of Social Security or National ID Numbers.** While some countries have national identity cards with unique numbers, there are often no systems equivalent to those used in the US for quick, inexpensive traces. It is normal practice for human resources departments to inspect original ID cards, driver's licenses, ration cards or passports during the hiring phase and to retain copies in personnel files.
- **Criminal Background Records.** Many countries do not have a national database for criminal background checks. Instead, searches must be compiled based on interviews and record checks in the different locations where the individual resided. In addition, some countries require a consent form signed by the candidate to accompany any requests for information.
- **Credit Checks.** Credit checks are a common component of US searches; however credit check information varies around the world. In some countries, use of consumer credit reporting is restricted to credit grantors and cannot be used for employment purposes. Where credit checks are available, information provided may be much less comprehensive than US credit checks and generally results in a report of "no information found."
- **Due Diligence on the Background Screening Agency.** Given increased security concerns and requirements for maintaining the privacy of customer information, background checks have

become more prevalent. The screening business has seen exponential growth.<sup>5</sup> Given the prevalence of online databases, entering this field is relatively easy. Financial institutions may choose to identify qualified background screeners from which the service provider must choose. Due diligence is essential.

- **Turnaround Time.** Many regions do not have online systems for public record searches and education and employment verification. In these areas, background checks are conducted manually. Relationships with universities must be developed over long time periods in order to ensure a timely response. In addition, corporate human resources departments in some regions do not have processes in place to reply to verification requests quickly. Screening companies may spend considerable time explaining who the company making the request is, what you want to do, and why.

---

<sup>5</sup>Background screening is estimated to be a two billion dollar business. See “Background Screening and Consumer Reports,” *Privacy and American Business*, April 2004.

**APPENDIX I: COUNTRY MATRICES**

<b>BACKGROUND SCREENING : AVAILABILITY OF INFORMATION IN ASIA PACIFIC</b> (First Advantage-Quest Research : Updated 16th April 2005)							
	Educational/ Professional Check	Employment Checks	Credit Check (or local best practice) (Note 1)	Criminal Check	Limited / Alternative to Criminal Check	Conflict of Interest Search / Business Interests Search (Note 2)	Financial Regulatory Search (Note 3)
Australia	Yes	Yes	Bankruptcy Note 4	Yes Note 5	Yes Note 6	Yes	Yes
China	Yes	Yes	NA	Yes	Yes Note 6	NA	Yes
Hong Kong	Yes	Yes	Civil litigation and bankruptcy	NA Note 7	Yes Note 6	Yes	Yes
India	Yes	Yes	Limited Note 8	Yes Note 9	Yes Note 6	Yes (Limited)	Yes
Japan	Yes	Yes	Bankruptcy Note 10	NA Note 11	Yes Note 6	NA	Yes
Korea	Yes	Yes	Credit check	NA Note 12	Yes Note 6	NA	NA
Malaysia	Yes	Yes	Civil litigation & bankruptcy	NA	Yes Note 6	Yes	Yes

NA = Not available in this jurisdiction or legality is uncertain.

**BACKGROUND SCREENING : AVAILABILITY OF INFORMATION IN ASIA PACIFIC**  
 (First Advantage-Quest Research: Updated 16<sup>th</sup> April 2005)

Country	Educational/ Professional Check	Employment Check	Credit Check (or local best practice) (Note 1)	Criminal Check	Limited / Alternative to Criminal Check	Conflict of Interest Search / Business Interests Search (Note 2)	Financial Regulatory Search (Note 3)
Singapore	Yes	Yes	Civil litigation & bankruptcy	Yes Note 7	Yes Note 6	Yes	NA
Taiwan	Yes Note 13	Yes	Credit check	Yes Note 14	Yes Note 6	NA	NA
Philippines	Yes	Yes	Credit check	Yes Note 15	Yes Note 6	NA	NA
New Zealand	Yes	Yes	Credit check	Yes Note 16	Yes Note 6	Yes	Yes
Thailand	Yes	Yes	Civil litigation & bankruptcy	NA	Yes Note 6	NA	Yes
Indonesia	Yes	Yes	Bankruptcy (Limited)	NA	Yes Note 6	NA	Yes

NA = Not available in this jurisdiction or legality is uncertain.

## NOTES

<b>BACKGROUND SCREENING : AVAILABILITY OF INFORMATION IN ASIA PACIFIC</b> (First Advantage-Quest Research : Updated 16th April 2005)	
1.	Most countries in Asia either do not have a consumer credit system or the use of that system is restricted to credit grantors. We thus advise using the local practice in respect of information that attests to the financial responsibility of the Applicant. This will usually mean carrying out civil litigation and/or bankruptcy searches.
2.	Conflict of interest search will determine if the Applicant is on record with the local company registration body as being a company director, shareholder or business owner.
3.	Financial regulatory check involves a search of the public domain enforcement announcements or banned lists maintained by the main market regulator in the jurisdiction.
4.	Country: Australia Under the Australian Privacy Act it is illegal to access consumer credit information for employment purposes. Best local practice is to carry out a nationwide bankruptcy search.
5.	Country: Australia Check is a National Name Check with the police service and covers the entire country. Search takes around three weeks.
6.	Countries: Australia, China, Hong Kong, India, Japan, Korea, Malaysia, Singapore, Taiwan, Philippines, New Zealand, Thailand, Indonesia A Limited Criminal Check consists of a combination of a local language press search for information pertaining to the arrest and/or conviction of the Applicant plus an IntegraScreen search. IntegraScreen is an enhanced due diligence database system with a high level of Asian content. IntegraScreen databases include all the major international proscribed lists (including OFAC, FBI, UN and the terrorism lists) plus proprietary databases such as Asian Fraud and Corruption, Asian Money Laundering, Asian Fraud Risk and Asian Stolen Passports. The utilization of these checks mitigate the risks that exist due to the inaccessibility and inadequacy of criminal records in the region. First Advantage-Quest Research is the exclusive background screening partner of IntegraScreen in the Asia Pacific region.
7.	Countries: Hong Kong, Singapore Third party criminal record checks are not available from police or courts (even with authorization). Certificates of No Criminal Conviction are issued to individuals for visa/emigration/adoption purposes only. Letters from foreign embassies must be provided (thus such certificates cannot be obtained for employment purposes).
8.	Country: India First Advantage-Quest Research has built a proprietary database of all major court decisions of the Supreme Court, all the High Courts and other quasi-judicial bodies since 1950. This covers Direct & Indirect Taxes, Company Law, SEBI Act & Labor Law. This would, however, represent a limited civil litigation search only.

9.	<p>Country: India</p> <p>Criminal Record Checks in India essentially involve obtaining local criminal record information (equivalent to Country Court records in the US) from the police office having jurisdiction over the Applicant's residential address.</p> <p><i>Procedure</i></p> <p>The procedure entails submitting a duly completed Personal Particulars Form of the Applicant along with relevant identification documents to the local police station or a centralized department in the city or town of residence – normally the Criminal Investigations Department (though this varies according to region). The police authorities then check the individual against records in their office and subsequently confirm whether a record exists or not.</p> <p>Note: procedures being followed differ from region to region and in fact there are minor variances between the various police stations within a particular region itself. This is mainly attributable to the fact that in India criminal records are not computerized in most places and consequently, centralized databases are not available either in the public domain or to the police authorities. As such local police stations are in a position to only verify the antecedents of an individual pertaining to their area of jurisdiction and not for the other locations the Applicant could have been residing in at an earlier date. Technically, any police file on an individual should move from location to location as the person moves, however in practice this does not happen.</p> <p>Multinational companies in India use criminal record checks for compliance purposes only as criminal records are rarely located due to a combination of poor record keeping procedures and corruption.</p>
10.	<p>Country: Japan</p> <p>Credit information cannot be accessed due to privacy legislation (enacted 2003).</p>
11.	<p>Country: Japan</p> <p>Third party criminal record checks are not available from police or courts (even with authorization). Police Clearance Certificates are issued to individuals if they apply in person. However, in support of their application they must supply “any document that shows good grounds for the necessity of the certificate”. The definition of such a document is an official document issued by a public organization e.g. a foreign embassy – not from a private organization or a lawyer. Thus, such certificates are not usually issued for employment purposes.</p>
12.	<p>Country: Korea</p> <p>Applicants can personally apply for a Korean Criminal History from any police station. This is issued for any purpose on payment of a small fee (around US\$10 – depending on the exchange rate). Third parties cannot apply for such a certificate. Please note that it is very common for prospective employers in Korea to ask applicants for such a certificate.</p>

13.	<p>Country: Taiwan Some financial accreditation bodies will not verify professional membership or status.</p>
14.	<p>Country: Taiwan In Taiwan a citizen or resident can apply for a Police Criminal Record Certificate at any major police station. However the police must inspect the Applicant's original national ID card. The Applicant also has to provide a copy of his national ID card together with the application form. The certificate will be issued in three working days if no records, or possible records, are found. The Applicant can request the police to send the certificate directly to a third party.</p>
15.	<p>Country: Philippines Criminal checks are conducted with the National Bureau of Investigation (Central Identification, Records and Statistics Division). The NBI receives records from the local courts, prosecutors' office and complaints directly filed with the NBI. As mandated by law, the NBI is the official depository of the records ( i.e. resolutions, information, decisions, warrant of arrest, recall of warrant of arrest etc.) from the courts and other judicial bodies (Sandiganbayan, Ombudsman and Tanodbayan). Also, some members of Interpol forward information about persons with derogatory records - particularly those who are subject for deportation or extradition orders and who they believe are hiding in the Philippines. However, it should be noted that there are some courts which are recalcitrant in forwarding their records to NBI, thus it is possible that a person has no records with the NBI but does have cases pending with the courts. NBI records go back over twenty years.</p> <p>Please note that few identifiers are found in the records thus further investigation can be very difficult in the event of a name match (which is not uncommon as so many Filipinos share common names).</p> <p>The most common practice by all employers in The Philippines is to ask job applicants to personally furnish an NBI clearance certificate at the time they apply for a job.</p>
16.	<p>Country: New Zealand The check is conducted via the Ministry of Justice, New Zealand, and covers the entire country.</p> <p>The records held by the Ministry of Justice include :-</p> <ul style="list-style-type: none"> <li>• Criminal and traffic convictions that have been processed through the Courts, including Youth Court charges where the charges have been proved</li> <li>• Custodial and non-custodial sentences</li> <li>• Cases/charges which are pending and not yet completed</li> </ul>

## BACKGROUND SCREENING : AVAILABILITY OF INFORMATION IN EUROPE

(Kroll: June 2005\*)

Y = information is available      N = information is not available

Countries	Emp Referenc es	Emp Verifica tion	Pers Referenc es	Edu Verifica tion	Addres s checks	CCJ	Bankrupt cy	Credit Checks	Prof. Certific ate	Director Appointme nts	Director Disqualific ations	Polic e Chec ks	Terrori sm	ID Checks	Country classification
Austria	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	RU	No	Yes	International core
Belgium	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	RU	No	No	International non core
Bosnia	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	RU	Yes	Yes	International non core
Bulgaria	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	RU	Yes	No	International non core
Croatia	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	RU	Yes	No	International non core
Czech Rep	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No	No	RU	Yes	Yes	International non core
Cyprus	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No	
Denmark	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	International core
Finland	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	Yes	International core
France	Yes	Yes	Yes	Yes	Basic level	Basic level	No	No	Yes	Yes	No	RU	No	No	International non core
Germany	Yes	Yes	Yes	Yes	Yes	No	No	Yes	RU	Yes	No	RU	No	No	International core
Hungary	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	Yes	RU	Yes	No	International core
Ireland	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No	International core
Italy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	RU	No	No	International core
Luxembo urg	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	RU	No	No	International core
Netherlan ds	Yes	Yes	Yes	Yes	RU	No	Yes	Yes	Yes	Yes	No	RU	No	No	International core
Norway	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No	International non core
Poland	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No	No	RU	Yes	No	International core
Portugal	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes	No	No	No	No	International non core
Russia	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No	No	No	No	International non core
Spain	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	RU	No	No	International core
Sweden	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	RU	No	Yes	International core
Switzerlan d	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes	No	RU	No	No	International core
Turkey	Yes	Yes	Yes	Yes	No	NO	Yes	No	Yes	No	No	No	Yes	No	International non core
UK	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	International core

RU - Candidate must request himself

## BACKGROUND SCREENING: AVAILABILITY OF INFORMATION IN North and South America

(Kroll: June 2005\*)

Y = information is available

N = information is not available

Countries	Emp Refs	Emp Verifs	Personal Refs	Edu Verific	Credit	Address	Police Checks	Prof Cert Verif	Director Apps	Directorship Disqualifs	Land Reg	Media	ID Checks	Country classification
Mexico	Y	Y	Y	Y	limited	limited	RU	Y	limited	limited	limited	Y	Y	International non core
Guatemala	Y	Y	Y	Y	basic	limited	RU	Y	N	N	limited	Y	Y	International non core
Honduras	Y	Y	Y	Y	N	N	RU	Y	N	N	N	basic	N	International non core
El Salvador	Y	Y	Y	Y	N	N	RU	Y	N	N	N	basic	N	International non core
Nicaragua	Y	Y	Y	Y	N	limited	RU	Y	N	N	N	basic	N	International non core
Costa Rica	Y	Y	Y	Y	basic	limited	RU	Y	N	N	limited	basic	Y	International non core
Panama	Y	Y	Y	Y	N	N	RU	Y	N	N	N	basic	Y	International non core
DR	Y	Y	Y	Y	N	N	RU	Y	N	N	N	basic	Y	International non core
Trinidad	Y	Y	Y	Y	N	N	RU	Y	N	N	N	basic	Y	International non core
Venezuela	Y	Y	Y	Y	N	limited	RU	Y	N	N	limited	basic	Y	International non core
Colombia	Y	Y	Y	Y	basic	limited	RU	Y	limited	limited	limited	basic	Y	International non core
Ecuador	Y	Y	Y	Y	basic	limited	RU	Y	limited	limited	limited	basic	Y	International non core
Peru	Y	Y	Y	Y	basic	limited	RU	Y	limited	limited	limited	basic	Y	International non core
Bolivia	Y	Y	Y	n	N	limited	RU	Y	N	N	N	basic	Y	International non core
Paraguay	Y	Y	Y	Y	N	limited	RU	Y	N	N	N	Y	Y	International non core
Uruguay	Y	Y	Y	Y	Y	limited	RU	Y	limited	limited	limited	Y	Y	International non core
Argentina	Y	Y	Y	Y	Y	Y	RU	Y	Y	Y	limited	Y	Y	International core
Brazil	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	limited	Y	Y	International core
Chile	Y	Y	Y	Y	limited	limited	RU	Y	limited	Y	limited	Y	Y	International non core
Columbia	Y	Y	Y	Y										
Canada	Y	Y	Y	Y	Y	Y	Y	RU	Y	Y	Y	Y	Y	International core
USA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	International core

**RU**

Candidate must request himself

**limited**

limited to some cities/some companies/too expensive or not reliable information

**basic**

Credit information limited to bankruptcy or basic information / media searches limited to major newspapers and recent issues.

## BACKGROUND SCREENING: AVAILABILITY OF INFORMATION IN AFRICA AND MIDDLE EAST

(Kroll: June 2005\*)

Y = information is available

N = information is not available

Countries	Employment Verification	Education Verification	Credit Checks	Police Checks	Bankruptcy Checks(on individuals)	Police Checks	Prof Cert Verif	Director Apps	Directorship Disqualifs	Land Reg	Media	Country classification
Algeria	Yes	Yes	No	No	N	N	Y	Y	N	Y	Y	International non core
Angola	Yes	Yes	No	No	Y	N	Y	N	Y	Y	Y	International non core
DR Congo	Yes	Yes	No	No	Y	Y	Y	Y	Y	N	N	International non core
Dubai	Yes	Yes	No	No	N	N	Y	N	N	N	Y	International non core
Egypt	Yes	Yes	No	No	Y	N	Y	Y	N	Y	N	International non core
Ghana	Yes	Yes	No	Yes	N	N	Y	N	Y	Y	Y	International non core
Iran	Yes	Yes	No	No	Y	N	Y	Y	Y	N	Y	International non core
Iraq	No	No	No	No	N	N	Y	N	N	Y	Y	International non core
Kenya	Yes	Yes	No	Yes	N	N	Y	Y	N	N	N	International non core
Lebanon	Yes	Yes	No	No	N	N	Y	N	N	N	N	International non core
Morocco	Yes	Yes	No	No	N	N	Y	N	N	N	Y	International non core
Nigeria	Yes	Yes	No	No	N	N	Y	N	N	N	N	International non core
Saudi/Gulf	Yes	Yes	No	No	N	N	Y	N	N	Y	Y	International non core
Sierra Leone	Yes	Yes	No	No	N	N	Y	N	N	N	Y	International non core
South Africa	Yes	Yes	CCJs and Bankrupcy	Yes	Y	Y	Y	Y	Y	Y	Y	International core
Tunisia	Yes	Yes	No	No	N	N	Y	N	N	N	Y	International non core
UAE	Yes	Yes	No	No	N	N	Y	N	N	N	Y	International non core
Zimbabwe	Yes	Yes	No	No	N	N	Y	N	Y	N	Y	International non core

\*©2003 Kroll Inc. All rights reserved. No portion of this work may be reproduced in any form without the prior written permission of the copyright holder. Kroll PRM is a trademark of Kroll Inc. This information is for general guidance only, whilst every effort has been made to ensure accuracy, Kroll PRM will not be held liable for any errors or omissions.

## **APPENDIX II: ABOUT THE AUTHORS**

### **About BITS**

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to [www.bitsinfo.org](http://www.bitsinfo.org).

BITS  
1001 PENNSYLVANIA AVENUE, NW  
SUITE 500 SOUTH  
WASHINGTON, DC 20004  
202-289-4322  
WWW.BITSINFO.ORG

### **About Kroll Worldwide**

Kroll Background America, Inc. (KBA), a wholly-owned subsidiary of Kroll Inc., is one of the country's leading private investigative companies. KBA, headquartered in Nashville, Tennessee, employs over 225 professionals and investigative staff. Kroll Inc. is the investigative subsidiary of Marsh & McLennan Companies, Inc. (NYSE: MMC).

### **About First Advantage-Quest Research**

First Advantage-Quest Research is the leading provider of background screening services in the Asia Pacific region and is a subsidiary of First Advantage Corporation (NASDAQ; FADV) a leading United States-based risk mitigation and business solutions provider. In Asia they run comprehensive screening programs for over two hundred companies with a large presence in the region including many US multinationals. They have offices in Hong Kong, Beijing, Singapore, Perth, Mumbai, Delhi, Chennai, Bangalore, and Dubai. They are a member of the National Association of Professional Background Screeners (USA) and have a full time staff of over 400. Further details can be found at [www.questresearch.com](http://www.questresearch.com).