Contract Endorsement

Unique Market Reference: **B0180PH1433938**

Endorsement Reference: **014**

Insured: **Alliant Property Insurance Program (APIP)**

CONTRACT CHANGES

Underwriters hereon note and agree that, effective 01 July 2014, **Slip Endorsement 001** is cancelled and replaced with the following:

Underwriters hereon note and agree that, effective 01 July 2014, the **PRIVACY BREACH RESPONSE SERVICES ENDORSEMENT** is added to the policy as follows:

PRIVACY BREACH RESPONSE SERVICES ENDORSEMENT

This endorsement modifies insurance provided under the following:

BEAZLEY BREACH RESPONSE

In consideration of the additional premium of USD 270,000.00 (excluding any applicable surplus lines taxes and fees), it is hereby understood and agreed that solely with respect to a **Claim** or incident arising out of the acts or operations of:

California State University Risk Management Authority (CSURMA)
The State of California as respects the Trustees of the California State University
The California State University (CSU)
Auxiliary Organizations of the California State University

1. Item 4.B. of the Declarations is deleted in its entirety.
2. Items 5.A.2, 5.B.2 and 5.C.2. of the Declarations are deleted in their entirety.
3. Item 4. of the Declarations is amended to include the following:

BBR. **LIMITS OF COVERAGE FOR PRIVACY BREACH RESPONSE SERVICES:**

1. **Notified Individuals** Limit of Coverage: 2,000,000 **Notified Individuals** in the aggregate

AGREEMENT

GENERAL UNDERWRITERS AGREEMENT (GUA) Each Underwriter's proportion is several not joint		
Slip Leader Only	Slip Leader and Agreement Parties	All Underwriters
Box 1	Box 2	Box 3

Note: Where more than one insurer participates in the contract, the contract terms may mean that it is not always necessary to obtain a record of agreement to the Contract Endorsement from all of those insurers.

DR

A sublimit of up to 10% of the **Notified Individuals** Limit of Coverage applies to **Notified Individuals** residing outside of the United States, which amount is part of and not in addition to the **Notified Individuals** Limit of Coverage

2. Aggregate Limit of Coverage for all **Computer Expert Services**, **Legal Services** and **Public Relations and Crisis Management Expenses** combined: USD 1,000,000

Coverage for all **Privacy Breach Response Services** is separate from and in addition to the **Policy Aggregate Limit of Liability.**

4. Item 5. Of the Declarations is amended to include the following:

BBR. **Privacy Breach Response Services**
Threshold and Retention:

1. **Notification Services**, **Call Center Services**, and **Breach Resolution and Mitigation Services** for each incident involving at least: 250 **Notified Individuals**
2. **Retention** applicable to **Computer Expert Services**, **Legal Services** and **Public Relations and Crisis Management Expenses**: USD 20,000 combined, but USD 5,000 for **Legal Services** (which retention is part of and not in addition to the combined retention)

5. Item 9. Of the Declarations is amended to include the following:

BBR. Privacy Breaches under Insuring Agreement B.:

Email: bbr.claims@beazley.com
Toll-Free 24-Hour Hotline: (866) 567-8570
(Emails and call reports from the toll-free hotline are forwarded to the Breach Response Services Team for response)

6. Endorsement No. 6., BEAZLEY NOMINATED VENDORS ENDORSEMENT shall not apply.

7. Insuring Agreement I.B. is deleted in its entirety and replaced with the following:

B. **Privacy Breach Response Services**

To provide **Privacy Breach Response Services** to the **Insured Organization** in excess of the **Retention** because of an incident (or reasonably suspected incident) described in Insuring Agreement I.A.1. or I.A.2. that first takes place on or after the **Retroactive Date** and before the end of the **Policy Period** and is discovered by the **Insured** and is reported to the Underwriters during the **Policy Period**.

Privacy Breach Response Services means the following:

1. **Computer Expert Services**;
2. **Legal Services**;
3. **Notification Services** to provide notification to:
   (a) individuals who are required to be notified by the **Insured Organization** under the applicable **Breach Notice Law**; or
   (b) in the Underwriters' discretion, individuals affected by an incident in which their **Personally Identifiable Information** has been subject to theft, loss or **Unauthorized Disclosure** in a manner which compromises the security or privacy of such individual by posing a significant risk of financial, reputational or other harm to the individual;
4. **Call Center Services**;
5. **Breach Resolution and Mitigation Services**; and

6. **Public Relations and Crisis Management Expenses**.

Privacy Breach Response Services also includes assistance from the BBR Services Team and access to educational and loss control information at no charge.

Privacy Breach Response Services will be provided subject to the terms and conditions of this Policy and the **Information Packet**, will be subject to the applicable retentions and limitations set forth in the Declarations, and shall not include any internal salary or overhead expenses of the **Insured Organization**.

8. Clause II., Defense and Settlement of Claims, paragraph B. is deleted in its entirety and replaced with the following:

B. With respect to any **Claim** against the **Insured** seeking **Damages** or **Penalties** which are payable under the terms of this Policy, the Underwriters will pay **Claims Expenses** incurred with their prior written consent. The Limit of Liability available to pay **Damages** or **Penalties**, or shall be reduced and may be completely exhausted by payment of **Claims Expenses**. **Damages**, **Penalties**, and **Claims Expenses** shall be applied against the **Retention** payable by the **Insured**.

9. Clause V., EXCLUSIONS, paragraphs B., J., K. and N. are deleted in their entirety and replaced with the following:

B. For, arising out of or resulting from any employer-employee relations, policies, practices, acts or omissions, or any actual or alleged refusal to employ any person, or misconduct with respect to employees, whether such **Claim** is brought by an employee, former employee, applicant for employment, or relative or domestic partner of such person; provided, however, that this exclusion shall not apply to an otherwise covered **Claim** under Insuring Agreements I.A.1., I.A.2., or I.A.3. by a current or former employee of the **Insured Organization**; or to the providing of **Privacy Breach Response Services** involving current or former employees of the **Insured Organization**;

J. For, arising out of or resulting from any of the following:

1. any actual or alleged violation of the Organized Crime Control Act of 1970 (commonly known as Racketeer Influenced and Corrupt Organizations Act or RICO), as amended, or any regulation promulgated thereunder or any similar federal law or legislation, or law or legislation of any state, province or other jurisdiction similar to the foregoing, whether such law is statutory, regulatory or common law;

2 any actual or alleged violation of any securities law, regulation or legislation, including but not limited to the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Act of 1940, any state or provincial blue sky or securities law, any other federal securities law or legislation, or any other similar law or legislation of any state, province or other jurisdiction, or any amendment to the above laws, or any violation of any order, ruling or regulation issued pursuant to the above laws;

3. any actual or alleged violation of the Fair Labor Standards Act of 1938, the National Labor Relations Act, the Worker Adjustment and Retraining Act of 1988, the Certified Omnibus Budget Reconciliation Act of 1985, the Occupational Safety and Health Act of 1970, any similar law or legislation of any state, province or other jurisdiction, or any amendment to the above law or legislation, or any violation of any order, ruling or regulation issued pursuant to the above laws or legislation; or

4. any actual or alleged discrimination of any kind including but not limited to age, color, race, sex, creed, national origin, marital status, sexual preference, disability or pregnancy;

However, this exclusion does not apply to any otherwise covered **Claim** under Insuring Agreements I.A.1., I.A.2., or I.A.3., or to paying **Privacy Breach Response Services** covered under Insuring Agreement I.B., that results from a theft, loss or **Unauthorized Disclosure** of **Personally Identifiable Non-Public Information**, provided that no member of the **Control Group** participated, or is alleged to have participated or colluded, in such theft, loss or **Unauthorized Disclosure**;

K. For, arising out of or resulting from any actual or alleged acts, errors, or omissions related to any of the **Insured Organization's** pension, healthcare, welfare, profit sharing, mutual or investment plans, funds or trusts, including any violation of any provision of the Employee

Retirement Income Security Act of 1974 (ERISA) or any similar federal law or legislation, or similar law or legislation of any state, province or other jurisdiction, or any amendment to ERISA or any violation of any regulation, ruling or order issued pursuant to ERISA or such similar laws or legislation; however this exclusion does not apply to any otherwise covered **Claim** under Insuring Agreements I.A.1., I.A.2., or I.A.3., or to the providing of **Privacy Breach Response Services** under Insuring Agreement I.B., that results from a theft, loss or **Unauthorized Disclosure** of **Personally Identifiable Non-Public Information**, provided that no member of the **Control Group** participated, or is alleged to have participated or colluded, in such theft, loss or **Unauthorized Disclosure**;

N. For, in connection with or resulting from a **Claim** brought by or on behalf of the Federal Trade Commission, the Federal Communications Commission, or any other state, federal, local or foreign governmental entity, in such entity's regulatory or official capacity; provided, this exclusion shall not apply to an otherwise covered **Claim** under Insuring Agreement I.C., or to the providing of **Privacy Breach Response Services** under Insuring Agreement I.B. to the extent such services are legally required to comply with a **Breach Notice Law**;

10. Clause V., EXCLUSIONS is amended to include the following:

BBR-A. For, arising out of or resulting from any liability or obligation under a **Merchant Services Agreement** except this exclusion does not apply to Insuring Agreement I.A.6., or to **Computer Expert Services** or **Legal Services** covered under Insuring Agreement I.B.;

11. Clause VI., DEFINITIONS, paragraph N., "Loss" is amended to replace "**Privacy Notification Costs**" with "**Privacy Breach Response Services**".

12. Clause VI., DEFINITIONS, is amended to include the following:

BBR-A. **Breach Resolution and Mitigation Services** means a credit monitoring, identity monitoring or other solution selected from the products listed in the **Information Packet** and offered to **Notified Individuals**. The product offered to **Notified Individuals** will be selected by the Underwriters in consultation with the **Insured Organization** and in accordance with the guidance provided in the Breach Resolution and Mitigation section of the **Information Packet**.

The product offer will be included in the communication provided pursuant to Insuring Agreement I.B.3.

BBR-B. **Call Center Services** means the provision of a call center to answer calls during standard business hours for a period of ninety (90) days following notification (or longer if required by applicable law or regulation) of an incident for which notice is provided pursuant to Insuring Agreement I.B.3. (Notification Services). Such notification shall include a toll free telephone number that connects to the call center during standard business hours. Call center employees will answer questions about the incident from **Notified Individuals** and will provide information required by the HIPAA/Health Information Technology for Economic and Clinical Health Act ("HITECH") media notice or by other applicable law or regulation.

Call Center Services will include up to 10,000 calls per day and will be provided in accordance with the terms and conditions set forth in the **Information Packet**. **Call Center Services** will be provided by a service provider selected by the Underwriters in consultation with the **Insured Organization** from the list of service providers in the **Information Packet**.

BBR-C. **Computer Expert Services** means costs for:

1. a computer security expert to determine the existence and cause of an actual or suspected electronic data breach which may require the **Insured Organization** to comply with a **Breach Notice Law** and to determine the extent to which such information was accessed by an unauthorized person or persons; and

2. a PCI Forensic Investigator that is approved by the PCI Security Standards Council and is retained by the **Insured Organization** in order to comply with the terms of a **Merchant Services Agreement** to investigate the existence and extent of an actual or suspected compromise of credit card data; and in the Underwriters' discretion, where a computer security expert described in 1. above has not been retained, for a computer security expert to provide advice and oversight in connection with the investigation conducted by the PCI Forensic Investigator; and

3. a computer security expert, up to USD 50,000 (which amount is part of and not in addition to the sublimit of coverage stated in Item 4.BBR.2. of the Declarations), to demonstrate the **Insured's** ability to prevent a future electronic data breach as required by a **Merchant Services Agreement**.

Computer Expert Services will be provided in accordance with the terms and conditions set forth in the **Information Packet** and will be provided by a service provider selected by the **Insured Organization** in consultation with the Underwriters from the list of service providers in the **Information Packet**.

BBR-D. **Information Packet** means the Information Packet provided with this endorsement. The **Information Packet** is incorporated into and forms part of this Policy and may be updated by the Underwriters from time to time.

BBR-E. **Legal Services** means fees charged by an attorney:

1. to determine the applicability of and actions necessary for the **Insured Organization** to comply with **Breach Notice Laws** due to an actual or reasonably suspected theft, loss or **Unauthorized Disclosure** of **Personally Identifiable Information**;

2. to provide necessary legal advice to the **Insured Organization** in responding to actual or suspected theft, loss or **Unauthorized Disclosure** of **Personally Identifiable Information**; and

3. to advise the **Insured Organization** in responding to credit card system operating regulation requirements for any actual or suspected compromise of credit card data that is required to be reported to the **Insured Organization's** merchant bank under the terms of a **Merchant Services Agreement**, but **Legal Services** does not include fees incurred in any actual or threatened legal proceeding, arbitration or mediation, or any advice in responding to credit card system operating regulations in connection with an assessment of **PCI Fines and Costs**.

Legal Services will be provided in accordance with the terms and conditions set forth in the **Information Packet** and will be provided by an attorney selected by the **Insured Organization** in consultation with the Underwriters from the list of attorneys in the **Information Packet**.

BBR-F. **Notification Services** means:

1. notification by first class mail or e-mail to United States or Canadian residents; and

2. notification by first class mail or e-mail to individuals residing outside the United States or Canada, but only to the extent reasonably practicable.

E-mail notification will be provided in lieu of first class mail to the extent reasonable, practicable and where permitted under the applicable **Breach Notice Law**. **Notification Services** will be provided by a service provider selected by the Underwriters in consultation with the **Insured Organization** from the list of service providers in the **Information Packet** and will be provided in accordance with the terms and conditions set forth in the **Information Packet**.

BBR-G. **Notified Individual** means an individual person to whom notice is given or attempted to be given under Insuring Agreement I.B.3. pursuant to a **Breach Notice Law**.

BBR-H. **PCI Fines and Costs** means the direct monetary fines, penalties, reimbursements, fraud recoveries or assessments owed by the **Insured Organization** under the terms of a **Merchant Services Agreement**, but only where such fines, penalties, reimbursements, fraud recoveries or assessments result both from the **Insured Organization's** actual or alleged noncompliance with published PCI Data Security Standards and from a data breach caused by an incident (or reasonably suspected incident) described in Insuring Agreement I.A.1. or I.A.2.; provided, that the term **PCI Fines, Expenses and Costs** shall not include or mean any charge backs, interchange fees, discount fees or prospective service fees.

BBR-I. **Public Relations and Crisis Management Expenses** shall mean the following costs approved in advance by the Underwriters in their discretion, and which are directly related to mitigating harm to the **Insured Organization's** reputation or potential **Loss** covered by the Policy resulting from an incident described in Insuring Agreement I.A.1. or I.A.2. or from a **Public Relations Event**:

1. costs incurred by a public relations or crisis management consultant;

2. costs for media purchasing or for printing or mailing materials intended to inform the general public about the incident, such costs to be limited to USD 100,000;

3. for incidents or events in which notification services are not otherwise provided pursuant to Insuring Agreement I.B., costs to provide notifications and notices via e-mail or first class mail to customers or patients where such notifications are not required by law ("voluntary notifications"), including to non-affected customers or patients of the **Insured Organization**;

4. costs to provide government mandated public notices related to breach events (including such notifications required under HITECH);

5. costs to provide services to restore healthcare records of **Notified Individuals** residing in the United States whose **Personally Identifiable Information** was compromised as a result of theft, loss or **Unauthorized Disclosure**; and

6. other costs approved in advance by the Underwriters.

Public Relations and Crisis Management Expenses must be incurred no later than twelve (12) months following the reporting of such **Claim** or breach event to the Underwriters and, with respect to clauses 1. and 2. above, within ninety (90) days following the first publication of such **Claim** or incident. If voluntary notifications are provided, e-mail notification will be provided in lieu of first class mail to the extent practicable.

BBR-J. **Public Relations Event** means the publication or imminent publication in a newspaper (or other general circulation print publication) or on radio, television or a publicly accessible website of a covered **Claim** under this Policy.

13. The second paragraph of Clause VII., LIMIT OF LIABILITY is deleted in its entirety.

14. Clause VII., LIMIT OF LIABILITY is amended to include the following:

BBR-A. The amount stated in Item 4.BBR.1. of the Declarations is the maximum total number of **Notified Individuals** to whom notification will be provided or attempted for all incidents or series of related incidents giving rise to an obligation to provide **Notification Services**, **Call Center Services** or **Breach Resolution and Mitigation Services**.

The aggregate limit of coverage stated in Item 4.BBR.2. of the Declarations is the aggregate limit of coverage for all **Computer Expert Services**, **Legal Services** and **Public Relations and Crisis Management Services** combined.

BBR-B. The Underwriters shall not be obligated to provide any **Privacy Breach Response Services** after the number of **Notified Individuals** under Insuring Agreement I.B.3. reaches an aggregate of the number of **Notified Individuals** stated in Item 4.BBR.1. of the Declarations. If the total number of individuals to be notified under the Policy exceeds the number of **Notified Individuals** stated in Item 4.BBR.1. of the Declarations, the **Insured** shall be responsible for providing notification, credit monitoring services or identity monitoring services to such additional individuals in accordance with Clause BBR-C. below.

BBR-C. If the total number of notifications made pursuant to Insuring Agreement I.B.3. aggregates to more than the number of notifications stated in Item 4.BBR.1. of the Declarations, the **Insured Organization** will be responsible for paying for **Privacy Breach Response Services** with respect to any excess notifications, and such costs will not be covered by the Policy. If an incident involves notifications made pursuant to Insuring Agreement I.B.3. both within the notification limit stated in Item 4.BBR.1. of the Declarations and in excess of such limit, all excess notifications will be provided by the same service provider that provides **Notification Services** covered under the Policy, and the costs will be allocated between the Underwriters and the **Insured Organization** pro rata based on the number of covered and non-covered notifications.

BBR-D. Unless otherwise specified in this Policy, **Privacy Breach Response Services** will be provided by the service providers listed in the **Information Packet**. In the event a service provider is unable to or does not provide the services set forth, the Underwriters will procure similar services from other sources; provided, the maximum the Underwriters will pay for the costs of procuring and providing all **Privacy Breach Response Services** under Insuring Agreement

I.B., including substitute products and services shall be no more than USD 10,000,000 in the aggregate for the **Policy Period**, which amount shall be in addition to the **Policy Aggregate Limit of Liability**. In the event there is a change of law, regulation or enforcement that prevents the Underwriters or its service providers from providing all or part of the **Privacy Breach Response Services**, the Underwriters will make reasonable efforts to substitute other services but, if this is not possible, the Underwriters shall not be obligated to provide such services.

15. Clause VIII., RETENTION, paragraphs B. and G. are deleted in their entirety and replaced with the following:

B. **Notification Services**, **Call Center Services**, and **Breach Resolution and Mitigation Services** will only be provided for each incident, event or related incidents or events, requiring notification to at least the number of individuals set forth in Item 5.BBR.1. of the Declarations. For incidents involving notification to fewer individuals there shall be no coverage for any such services under Insuring Agreement I.B.

For all **Computer Expert Services**, **Legal Services** and **Public Relations and Crisis Management Services**, the **Retention** amounts set forth in Item 5.BBR.2. of the Declarations apply separately to each incident, event or related incidents or events, giving rise to an obligation to provide such services; and the Each Incident **Retention** shall be satisfied by monetary payments by the **Named Insured** for such services.

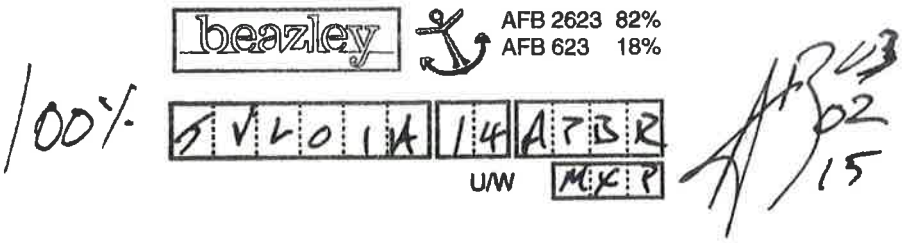
G. Satisfaction of the applicable **Retention** is a condition precedent to the payment by the Underwriters of any amounts hereunder, and the Underwriters shall be liable only for the amounts in excess of such **Retention** subject to the Underwriters' total liability not exceeding the **Policy Aggregate Limit of Liability** or any applicable Limit of Liability or Limit of Coverage for **Privacy Breach Response Services**. The **Named Insured** shall make direct payments within the **Retention** to appropriate other parties designated by the Underwriters.

16. Clause X., CONDITIONS, NOTICE OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM, paragraph A.2. is deleted in its entirety and replaced with the following:

2. With respect to Insuring Agreement I.B., for a legal obligation to comply with a **Breach Notice Law** because of an incident (or reasonably suspected incident) described in Insuring Agreement I.A.1. or I.A.2., such incident or reasonably suspected incident must be reported as soon as practicable during the **Policy Period** after discovery by the **Insured** via the email address or telephone number set forth in Item 9.BBR. of the Declarations; provided, that unless the **Insured** cancels the Policy, or the Underwriters cancel for non-payment of premium, incidents discovered by the **Insured** within sixty (60) days prior to expiration of the Policy shall be reported as soon as practicable, but in no event later than sixty (60) days after the end the **Policy Period**; provided further, that if this Policy is renewed by the Underwriters and **Privacy Breach Response Services** are provided because of such incident or suspected incident that was discovered by the Insured within sixty (60) days prior to the expiration of the Policy, and first reported during the sixty (60) day post **Policy Period** reporting period, then any subsequent **Claim** arising out of such incident or suspected incident is deemed to have been made during the **Policy Period**.

Notwithstanding the foregoing, if the **Named Insured** reasonably believes that the **Privacy Breach Response Services** provided as a result of such incident or suspected incident are not likely to meet or exceed the **Retention**, then reporting of such incident or suspected incident under this Clause X.A.2. is at the **Named Insured's** option, but unless such incident or suspected incident is reported in accordance with the first paragraph of this Clause X.A.2., there shall be no coverage for **Privacy Breach Response Services** in connection with such incident or suspected incident.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED.



London Dated: 03 February 2015

ATTACHMENT A

Campus Addresses

Office of the Chancellor
401 Golden Shore, Long Beach, CA 90802

California State University, Bakersfield
9001 Stockdale Highway, Bakersfield, CA 93311-1099

California State University, Channel Islands
One University Drive, Camarillo, CA 93012

California State University, Chico
1st and Normal Streets, Chico, CA 95929-0722

California State University, Dominguez Hills
1000 East Victoria Street, Carson, CA 90747

California State University, East Bay
25800 Carlos Bee Blvd., Hayward, CA 94542-3035

California State University, Fresno
5150 North Maple Avenue, Fresno, CA 93740-0057

California State University, Fullerton
800 North State College Boulevard, Fullerton, CA 92834-6900

Humboldt State University
1 Harpst Street, Arcata, CA 95521-4957

California State University, Long Beach
1250 Bellflower Blvd., Long Beach, CA 90840-0106

California State University, Los Angeles
5151 State University Drive, Los Angeles, CA 90032-8530

California Maritime Academy
200 Maritime Academy Drive
PO Box 1392, Vallejo, CA 94590

California State University, Monterey Bay
100 Campus Center Drive, Seaside, CA 93955-8001

California State University, Northridge
18111 Nordhoff Street, Northridge, CA 91330-8207

California State Polytechnic University, Pomona
3801 West Temple Ave., Pomona, CA 91768-4003

California State University, Sacramento
6000 J Street, Sacramento, CA 95819-6048

California State University, San Bernardino
5500 University Parkway, San Bernardino, CA 92407-2397

San Diego State University
5500 Campanile Drive, San Diego, CA 92182-7455

San Francisco State University
1600 Holloway Ave., San Francisco, CA 94132-4002

San Jose State University
One Washington Square, San Jose, CA 95192-0009

California Polytechnic State University, San Luis Obispo
San Luis Obispo, CA 93407

California State University, San Marcos
333 S. Twin Oaks Valley Road, San Marcos, CA 92096-0001

Sonoma State University
1801 East Cotati Ave., Rohnert Park, CA 94928-3609

California State University, Stanislaus
801 West Monte Vista Ave., Turlock, CA 95382

ATTACHMENT B

Auxiliary Organization

Associated Students, California State University, Bakersfield, Inc.
California State University, Bakersfield Auxiliary for Sponsored Programs and Administration
California State University, Bakersfield Foundation
California State University, Bakersfield Student Union, Inc.
California State University Foundation
California State University Institute
Associated Students of California State University, Channel Islands, Inc.
California State University Channel Islands Foundation
University Glen Corporation
Associated Students of California State University, Chico
Auxiliary Organization Associations
The CSU, Chico Research Foundation
The University Foundation, California State University, Chico
Associated Students, California State University, Dominguez Hills
California State University, Dominguez Hills Foundation
Donald P. and Katherine B. Loker University Student Union, Incorporated
Associated Students, California State University, East Bay
Cal State East Bay Educational Foundation
California State University, East Bay Foundation, Inc.
Associated Students, Inc. of California State University, Fresno
California State University, Fresno Association, Inc.
California State University, Fresno Foundation
Fresno State Programs for Children, Inc.
The Agricultural Foundation of California State University, Fresno
The California State University, Fresno Athletic Corporation
Associated Students, California State University, Fullerton, Inc.
Cal State Fullerton Philanthropic Foundation
CSU Fullerton Auxiliary Services Corporation
CSU Fullerton Housing Authority (will be dissolved by 6/30/14)
Associated Students, Humboldt State University
Humboldt State University Advancement Foundation
Humboldt State University Center Board of Directors
Humboldt State University Sponsored Programs Foundation
Associated Students, California State University, Long Beach
California State University, Long Beach Research Foundation
CSULB 49er Foundation
Forty-Niner Shops, Inc., CSU Long Beach

Associated Students, California State University, Los Angeles, Inc.
Cal State L.A. University Auxiliary Services, Inc.
California State University, Los Angeles Foundation
University-Student Union Board, California State University, Los Angeles
California Maritime Academy Foundation, Inc.
The Associated Students of the California Maritime Academy
Foundation of California State University, Monterey Bay
The University Corporation at Monterey Bay
Associated Students, California State University, Northridge, Inc.
California State University, Northridge Foundation
North Campus University Park Development Corporation
The University Corporation, CSU Northridge
University Student Union of California State University, Northridge
Associated Students Inc., California State Polytechnic University, Pomona
The Cal Poly Pomona Foundation, Inc.
Associated Students of California State University, Sacramento
Capital Public Radio, Inc., CSU Sacramento
The University Foundation at Sacramento State
University Enterprises, Inc., CSU Sacramento
University Union Operation of CSUS, Inc.
Associated Students Inc., California State University, San Bernardino
CSUSB Philanthropic Foundation
Santos Manuel Student Union of California State University, San Bernardino
University Enterprises Corporation at CSUSB
Associated Students, San Diego State University
Aztec Shops, Ltd., San Diego State University
San Diego State University Research Foundation
The Campanile Foundation
Associated Students, Inc., San Francisco State University
Cesar Chavez Student Center, San Francisco State University
San Francisco State University Foundation
The University Corporation, San Francisco State
Associated Student, San Jose State University
San Jose State University Research Foundation
Spartan Shops, Inc., San Jose State University
The Student Union of San Jose State University
The Tower Foundation, San Jose State University
Associated Students, Inc., California Polytechnic State University at San Luis Obispo
Cal Poly Corporation
California Polytechnic State University Foundation

California State University San Marcos Foundation

San Marcos University Corporation

The Associated Students of California State University, San Marcos

University Auxiliary and Research Services Corporation

Associated Students of Sonoma State University

Sonoma State Enterprises, Inc.

Sonoma State University Academic Foundation, Inc.

Associated Students, Inc., California State University, Stanislaus

California State University, Stanislaus Auxiliary and Business Services

California State University, Stanislaus Foundation

University Student Union of California State University, Stanislaus

Beazley Group | Beazley Breach Response

BBR

Information Pack



AFB
2623
623

Beazley Breach Response

Information Packet for privacy breach response and risk management services

Thank you for purchasing a Beazley Breach Response (BBR) insurance policy.

BBR is the industry leading solution for data privacy and security risk management, and provides a range of services designed to help your organization respond to an actual or suspected data breach incident effectively, efficiently, and in compliance with the law.

This Information Packet details the features of your BBR policy and sets out the process for responding to an actual or suspected data breach, including how to obtain the maximum benefit of Beazley's Breach Response Services team. We encourage you to circulate this Information Packet to the members of your data breach incident response team, and incorporate the resources available under the policy as a component of your incident response plan.



Your BBR policy includes an array of benefits and services including:

- Complimentary loss control and risk management information including online resources and value-added educational webinars (www.nodatabreach.com).
- A computer forensics "Information Security Incident Response" guide to empower your organization's IT staff with knowledge of crucial forensic procedures that can make or break the investigation of a suspected breach.
- Assistance at every stage of the investigation of, and response to, a data breach incident from Beazley's in-house BBR Services team of data privacy attorneys and technical experts.

A single call or email to BBR Services, notifying the team of a suspected data breach will begin activation of the following services:

Initial breach investigation and consulting

- Legal services
- Computer forensic services

Response to breach events

- Notification services including foreign notification where applicable
- Call center services
- Breach resolution and mitigation services
- Public relations and crisis management expenses

beazley

AFB
2623
623

Risk management tools and resources

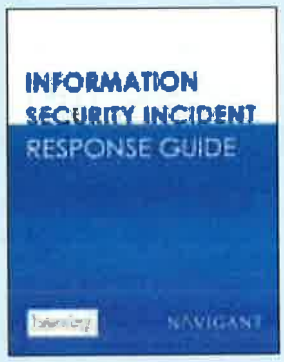
As a BBR policy holder, your organization is entitled to enroll in **nodatabreach.com**, an online service that provides educational and loss control information relating to compliance with applicable laws, safeguarding information, preparing to respond to breach incidents and best practices.

ePlace Solutions Inc. administers **nodatabreach.com** and will reach out to you by separate email to provide you information on accessing the website. If you enroll in **nodatabreach.com**, you will have the opportunity to attend webinars on current topics related to information security and breach preparedness, and be able to receive other risk management tools and information that we periodically make available to our policy holders.

Information Security Incident Response Guide

Beazley, in partnership with Navigant, a leader in complex data management and forensics analysis, developed a joint Information Security Incident Response Guide aimed at providing a roadmap for companies to prepare for and manage the aftermath of a data security breach. The guide, provided to BBR policyholders, addresses the increasing need for effective risk management on the part of companies hoping to limit the damage caused by a data breach.

The Information Security Incident Response Guide addresses information security incidents such as malware intrusions, social engineering attacks, unauthorized network access, lost or stolen devices, and other kinds of data security incidents and breaches. The guide also provides in-depth case studies and best practices for preparation, risk assessment, and incident documentation, highlighting the varied components of an effective response.





AFB
2623
623

Activation of breach response services

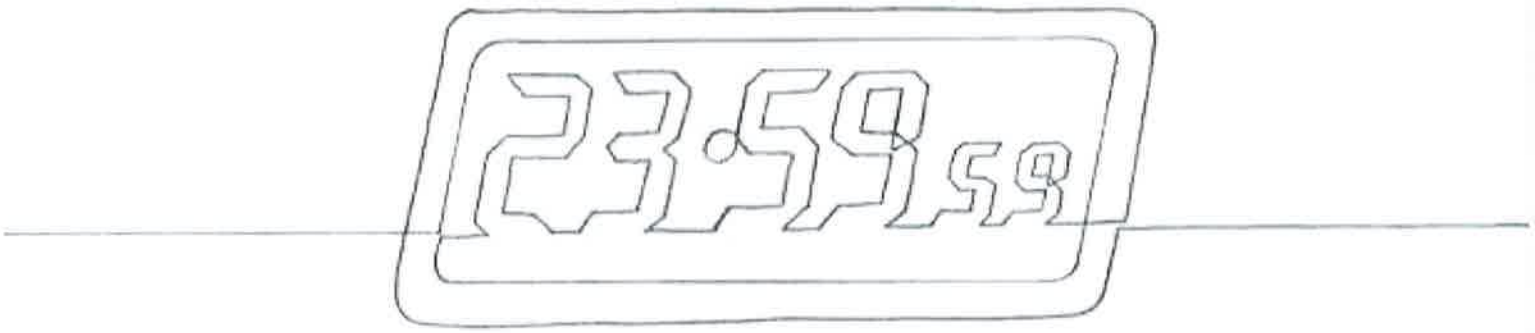
Beazley Breach Response Services Team

Beazley is committed to providing industry leading data breach response services for our clients. This is why we created the BBR Services team; a dedicated business unit within Beazley, focused exclusively on helping insureds successfully prepare for and respond to breaches. The BBR Services team works in collaboration with you to triage and assess the severity of a data breach incident, while coordinating the range of resources and services you may need to meet legal requirements and maintain customer confidence. BBR Services is your frontline partner in data breach investigation and response, and available to your organization regardless of the size, severity, or cost of a data breach.

When to notify us?

You should notify Beazley as soon as you suspect that personally identifiable or confidential data for which you are responsible might have been compromised. The sooner you notify us about a potential data breach, the more our BBR Services team can do to help.

It is also important that you contact us first before retaining any service providers as the BBR Services team will take you through the process and work with you to secure services from providers that best match your needs.



How to notify us?

Send an email to **bbr.claims@beazley.com** with the following in your notification email:

- the name of your organization and insurance policy number if possible;
- a short description of the incident;
- the date the incident occurred (if known);
- the date your organization discovered the incident; and
- contact information for the point person handling the investigation.

Do not:

- email Beazley staff directly to provide the initial notice; or
- include any personally identifiable information or protected health information.

Email is strongly recommended as the best method of notification; you may alternatively provide notice of an incident by calling Beazley's 24-hour hotline, (866) 567-8570, and provide the information described above.

What happens after notifying us?

A BBR Services team member will respond to the notice generally on the same or next business day and will schedule a phone call to discuss the incident, assist you with any needed breach investigation and response services available under your BBR policy. We recommend that those within your organization who are involved in investigating the incident participate on this phone call.

The BBR Services team will continue to collaborate with you throughout the investigation and response process, to provide guidance and to arrange breach investigation and response services provided by Beazley's network of expert service providers.

AFB 2623 623

Legal services

If an incident occurs that might require notification under relevant breach notice laws or regulations, specific Legal Services to assist you in investigating and responding to the incident are included in the Services.

BBR Services will arrange Legal Services for you and will connect you to these experts; please do not contact Beazley's partnering law firms directly without the involvement of BBR Services.

United States

Baker Hostetler LLP
Theodore J. Kobus III, Lynn Sessions, Craig A. Hoffman, Randal L. Gainer and Eric A. Packel
www.bakerlaw.com

McDonald Hopkins LLC
James J. Giszczak and William J. O'Neill
www.mcdonaldhopkins.com

InfoLaw Group LLP
David Navetta, Tanya Forsheit and Boris Segalis
www.infolawgroup.com

Vedder Price
Bruce A. Radke and Michael J. Waters
www.vedderprice.com

Buchanan Ingersoll & Rooney PC
Matt Meade and Jack Tomarchio
www.bipc.com

Lewis Brisbois Bisgaard & Smith LLP
John F. Mullen and Gordon J. Calhoun
www.lbbslaw.com

International

DAC Beachcroft LLP
Patrick Hill and Hans Allnut
www.dacbeachcroft.com

Dentons
Nick Graham
www.dentons.com

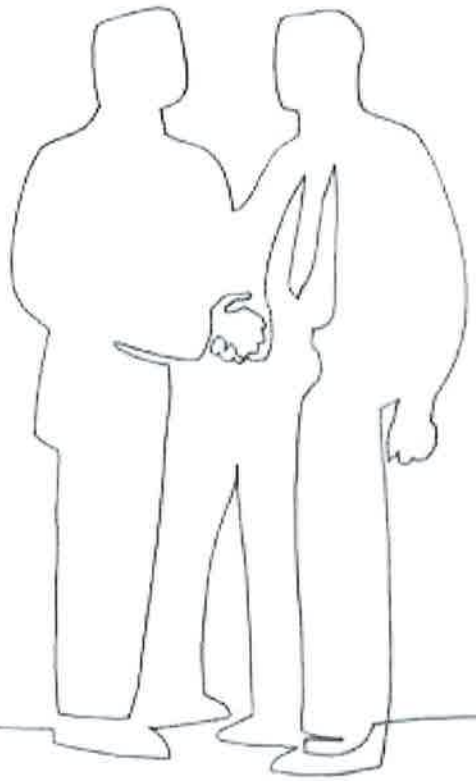
CMS Françis Lefebvre
Anne-Laure Villedieu
www.cms-cmck.com

Cotty Vivant Marchisio & Lauzeral
Guillaume Seligmann
www.cvml.com

Bird & Bird
Guillaume Raimbault
www.twobirds.com

CMS Adonnino Ascoli & Cavasola Scamoni
Laura Opilio
www.cms-aacs.com

Portolano Cavallo Studio Legale
Laura Liquori
www.potrolano.it



AFB 2623 623

Computer expert services

In the event that external forensics assistance is needed to assess the impact of a data incident on your computer system, Computer Expert Services will be provided to (1) help to determine whether, and the extent to which, notification must be provided to comply with Breach Notice Laws, and (2) if applicable, give advice and oversight in connection with the investigation conducted by a PCI Forensic Investigator.

The computer security expert that provides Computer Expert Services will require access to information, files and systems and it is important for you to comply with the expert's requests and cooperate with the investigation. Reports or findings of the expert will be made available to you, us, the BBR Services team and any attorney that you retain to provide advice with regard to the incident.

BBR Services will arrange Computer Expert Services for you and will connect you to these experts; please do not contact Beazley's partnering forensics firms directly without the involvement of BBR Services.

United States and Canada
Navigant Consulting, Inc.
www.navigant.com

Verizon Investigative Response Unit
www.verizonenterprise.com/products/security/risk-team/investigative-response.xml

Digital Forensics Solutions, LLC
www.digitalforensicssolutions.com

Kroll Ontrack
www.krollontrack.com

International
CGI
www.cgi.com

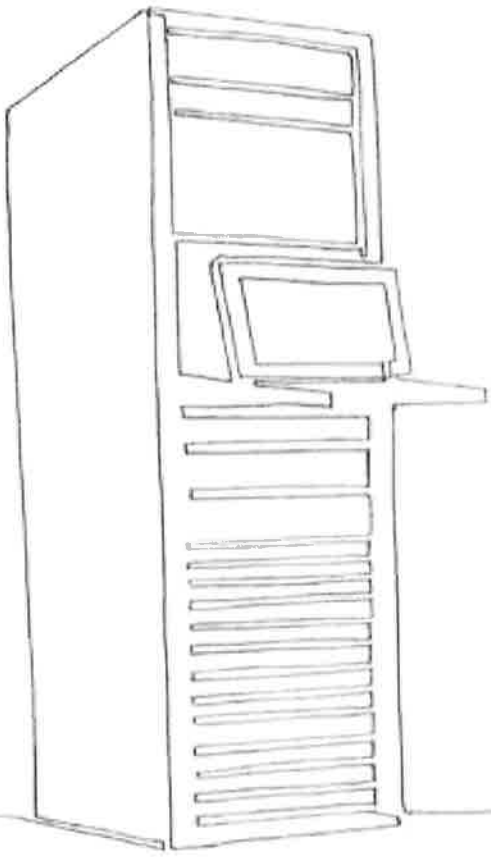
Navigant Consulting, Inc.
www.navigant.com

DF Labs
www.dflabs.com

Kroll Ontrack Legal Technologies Ltd
www.krollontrack.co.uk

Kroll Ontrack
www.ontrack.fr

Kroll Italia
www.ontrackdatarecovery.it



AFB 2623 623

Notification services and call center services

BBR Services will assist you with the notification process, including arranging for notification and/or call center service. BBR Services will walk you through notification details such as how to work with privacy counsel to develop notification letters and how to timely provide notification letters, relevant addresses and other required deliverables to the notification vendor.

Notification letters will be black and white and two-sided; returned mail will be provided to you at your request. Mailing may be staggered to accommodate the number of notifications and anticipated call center volume. For notifications by U.S. mail, the notification vendor will update and mail notifications according to the U.S. Postal Service data base of address changes. Notification services do not include further tracing of individuals whose notifications are returned.

BBR Services will also walk you through developing a set of frequently asked questions (FAQs) for use by the call center and how to anticipate and prepare for call escalations.

United States and Canada
Immersion, Ltd.
www.useinfolaunch.com

Epiq Corporate Services, Inc.
www.epiqcorporateservices.com

Intelligent Business Concepts, Inc.
www.intellbc.com

International
Call Center Services will be provided to individuals residing outside the United States or Canada to the extent reasonably practicable, and only where available through the international call center service provider(s) listed below or, in our discretion, in other jurisdictions and language where such services are reasonably available.

Baker Goodchild (Notification Services)
www.bakergoodchild.co.uk

D.P. Direct Mail Ltd (Notification Services)
www.dpdirect.co.uk

CGI (Call Center Services)
www.cgi.com



AFB 2623 623

Breach resolution and mitigation services

Beazley Breach Response includes a number of products that provide Resolution and Mitigation Services, including one and three bureau monitoring and identify monitoring solutions. All the solutions include fraud resolution services.* Based on our experience, three bureau credit monitoring is generally appropriate for breaches involving data such as names combined with social security numbers. For breaches involving less sensitive data, one bureau credit monitoring or identity monitoring solutions may be appropriate. The BBR Services team has handled over 1,000 data breaches and will advise you on which products or solutions may be applicable for a particular breach event.

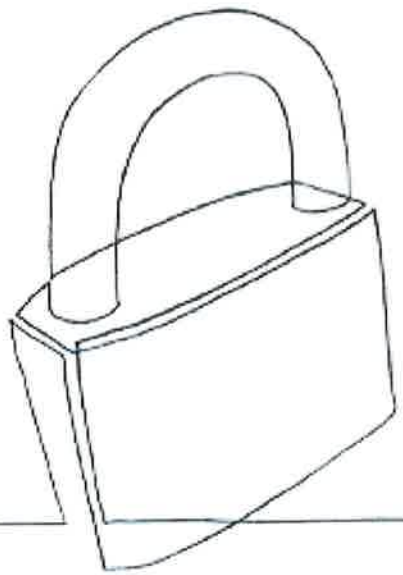
A product or solution may be offered where reasonably practicable and only to the extent available in a particular jurisdiction. Notified Individuals will have up to ninety (90) days from mailing of the notification to subscribe to an offered product or solution and they must qualify for enrollment, complete the enrollment process and agree to the applicable terms and conditions set by the provider. Enrollees of an offered product or solution will have access to the services provided under such product or solution for 12 months from the date of their enrollment.

Credit monitoring products

- ProtectMyID® Alert 3 Bureau Credit Monitoring Product
- ProtectMyID® Alert 1 Bureau Credit Monitoring Product
- Family Secure® credit monitoring product (for identified minors involved in the breach; to be offered through their parents or guardians)
- Experian Limited Credit History Service (a service offering for individuals with limited or no Experian credit history that monitors for the creation of an Experian credit file)
- Fraud resolution services are available to subscribers of the ProtectMyID® Alert or Family Secure® or the Experian Limited Credit History Solution,* who become victims of identity theft
- ProtectMyID® Alert, Family Secure®, the Experian Limited Credit History Solution and the fraud resolution services will be provided by ConsumerInfo.com, Inc., and/or its affiliated Experian companies
- Equifax Complete™ Advantage Plan (for Canadian residents only)
- Equifax Credit File ID Alert™ (for Canadian residents only)
- ProtectMyID™ provided by Experian Limited. (for UK residents only)

Identity monitoring products

- Experian DataPatrol™, offered by Experian Limited, including fraud support services for subscribers through ConsumerInfo.com, Inc.*



* Fraud resolution and fraud support services require that subscribers are eligible to enroll in ProtectMyID® or Family Secure® and complete such enrollment.

AFB 2623 623

Additional information on products and offerings

Descriptions of each of the credit or identity monitoring products and solutions and risk management tools are attached. Such descriptions are provided by ConsumerInfo.com, Inc., Equifax Canada Co., Experian Limited and ePlace Solutions Inc. and are for informational purposes only and are not part of the Policy. The actual services available with each product or solution are governed by the terms and conditions of the applicable agreements that you must enter into prior to the product or solution being offered to Notified Individuals. Further information about the ConsumerInfo.com and Equifax Canada products can be obtained at the telephone numbers indicated in the applicable description. You may also contact us through your insurance broker to receive additional information about the Services.

Your responsibilities

To ensure that the Services described above are provided promptly and properly, you must follow the requirements and procedures set forth in the Policy and in this Information Packet. We require your assistance and cooperation with us and with any third party vendors providing Services. Please respond to BBR Services or outside vendor requests and inquiries in a timely manner and enter into necessary contracts required by our vendors for the provision of services. You will be responsible for paying any costs resulting from your failure to timely provide responses, accurate information or approvals necessary for the provision of the Services. There is no coverage under the Policy for any of your internal salary or overhead expenses or for your assistance and cooperation in responding to a breach incident. In the event of a breach incident or suspected incident, do not contact any service providers directly. Instead, you must first provide notice to us at **bbr.claims@beazley.com** or at **(866) 567-8570**, as further described on page 3 of this Information Packet and also in Item 9.(b) of the Declarations.

Contacting any of the service providers listed in this Information Packet shall not constitute notice under the terms of the Policy.

As used in this Information Packet, the terms "we" or "us" or have the same meaning as the term "Underwriters" in the Policy and "you" has the same meaning as the "Insured Organization" in the Policy. Capitalized terms not defined in this Information Packet have the same meaning as set forth in the Policy.

Appendices

ProtectMyID® Alert

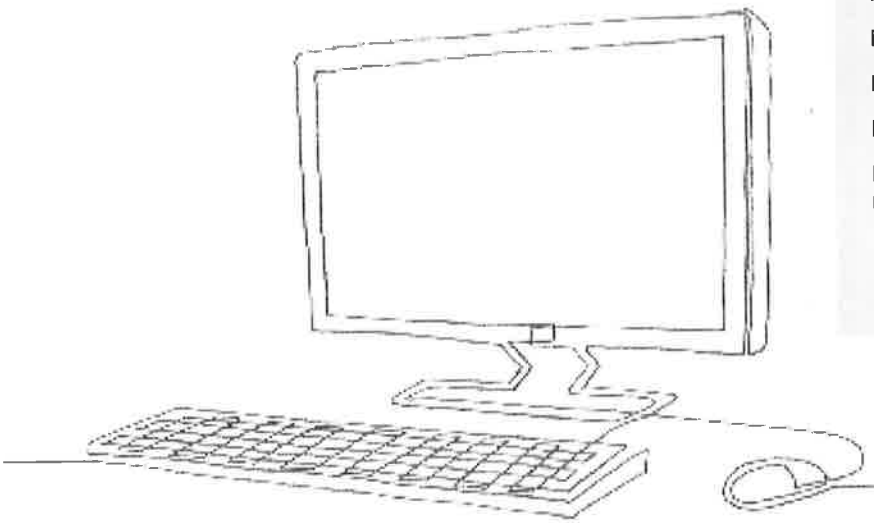
Family Secure®

Equifax Complete™ Advantage Plan

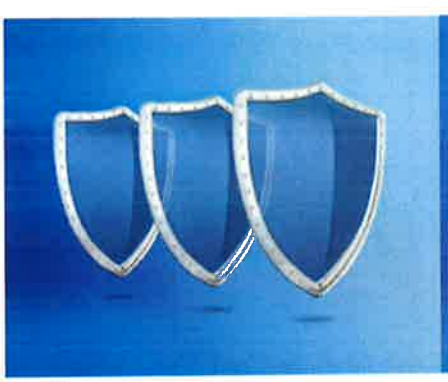
Equifax Credit File ID Alert™

Experian DataPatrol™

Data security risk management - nodatabreach.com



AFB 2623 623



ProtectMyID® Alert

All of the benefits of a multi-layered identity theft detection, protection, and resolution product with a focus on our fundamental services.

Experian℠

PROTECTmyID.com
A part of Experian

ProtectMyID Alert leverages the superior identity theft protection services of ProtectMyID with a focus on advanced features that help consumers identify and resolve identity theft before it escalates out of control.

Peace of mind in the face of sudden data loss

With the time it takes to resolve identity theft increasing to 40 hours in 2010 and the average individual's out of pocket expense growing to $631[1] the effects of a data breach can result in potential damage to your brand and loss of revenue. You can help to minimize the legal risks and financial costs associated with a data breach by partnering with Experian® to mitigate the effects of such adverse incidents. ProtectMyID's dedicated professionals manage your case and provide assistance throughout the entire process, helping you to maintain customer loyalty and strengthen your brand by resolving a data breach rapidly and discreetly.

Experience-driven protection

Experian has managed thousands of data breach incidents in the finance, education, commerce, medical, and government sectors. With our latest addition to the ProtectMyID family, ProtectMyID Alert, you can offer the same trusted name in identity theft protection while addressing your customers' or employees' immediate needs with credit monitoring, fraud resolution, and identity theft insurance.

Experian's finest identity theft protection and credit monitoring solution

ProtectMyID guards your employees' and customers' most valuable asset — their identity. What they experience is the same superior identity theft protection Experian has provided to millions of consumers and thousands of organizations. Ease of use. Peace of mind. Protection like no other.

Multiple levels of vital detection and support

Daily credit monitoring of up to 3 bureaus and timely alerts

- Early warning Surveillance Alerts[SM] notify members of key credit report changes covering 50 potential indicators of fraud.
- Information on new accounts, medical collections, and other activity allows members to understand when their identities may be at risk.
- Timely notification empowers members to quickly and efficiently respond to potential identity theft.

US-based Fraud Resolution Team

- Can help to investigate and address both credit and non-credit related fraud.
- Are highly trained professionals that can contact credit grantors to dispute charges, close accounts, and provide additional assistance as needed.

$1 Million Identity Theft Insurance[2]

- Provides coverage for lost wages, legal fees, and funds lost due to unauthorized electronic fund transfers.
- Zero deductible upon enrollment.

Experian credit report

- Members can check for past inaccuracies and signs of identity theft.

Additional educational resources

- Critical insight into identity protection and identity theft resolution.
- Medical identity theft resources in members online Protection Center include instructions on requesting a drug history report, deciphering a medical benefits statement, and looking into medical information disclosures.

[1] 2011 Identity Fraud Survey Report, Javelin Strategy & Research

[2] Insurance underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

©2010 Experian Information Solutions, Inc. All rights reserved. Experian and the marks used herein are service marks or registered trademarks of Experian Information Solutions, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners.

To learn more about ProtectMyID Alert and our Data Breach Resolution Solutions, call Experian at **1 866 751 1323** or visit **Experian.com/DataBreach**.

APR 2023 523



Family Secure®

Online credit monitoring with a $2 million guarantee protects families against fraud and identity theft.

Experian℠

Many competing services primarily rely on third party or partial data sets which may not report anything that impacts an individual's credit standing, which is the critical factor to monitor. In fact, if any issues related to the child's credit file arise, the competing services must work through the bureau to correct them.

Key Product Features & Benefits

- Monthly monitoring of Experian® information for **every** enrolled child in the family.
- Protection from material damages that may occur against a child whose credit file is misused.
- If no credit file exists, Experian monitors the child's personal information for the creation of one.
- Searches for important activity associated with the child including credit inquiries, public records, delinquencies, new accounts, and negative information (e.g., liens, civil judgments, bankruptcies.)
- Activity is detected based on the child's Social Security Number, date of birth, name and address utilizing Experian's proprietary credit file matching logic. This logic minimizes false positives.
- Email or mobile text alerts are sent to the parent/guardian if there is any new activity in the child's name.
- If activity is detected, the parent/guardian can work with a dedicated Experian Fraud Resolution representative on the best course of action to repair your child's identity.
- Provides monthly No Hit Alerts if no credit activity is detected.
- Comprehensive Fraud Resolution expertise – toll-free access to experienced, dedicated professionals who can manage your family's case and help your family recover from identify theft quickly and efficiently.
- Dedicated Fraud Resolution Agents work with your family to provide assistance throughout the fraud resolution process including assistance with freezing credit files, contacting creditors to dispute charges, closing accounts, compiling documents and contacting relevant government and law enforcement agencies.
- Daily monitoring of primary parent's credit report for 50 leading indicators of identity theft and early warning alerts if credit report changes are detected.
- Unlimited, on-demand access to Experian credit reports and scores 24/7.
- Experian credit score illustrator shows monthly score trending and analysis for the adult member.

EQUIFAX

CONSUMER INFORMATION SOLUTIONS

Corporate Data Breach Solutions

What is Credit Monitoring?

Equifax Complete™
Advantage Plan
key features

- **Online access** to view your Equifax credit report 24/7
- **Credit monitoring** with e-mail notification of key changes to your credit file
- **Updates** of your Equifax credit report and score once every three months
- **Dedicated** customer service

Equifax Canada Co. is Canada's largest credit reporting agency. A credit reporting agency is an independent organization that receives information from credit grantors and other (private and public) sources regarding individuals' credit activity. This information is compiled in a credit report for each Consumer.

Your credit report is a summary of your credit history. Your credit report contains information about your credit cards and loans, such as: when you opened your account, account balance, payment history, etc. Your credit report also includes personal information that is available in public records, such as a bankruptcy.

What is Credit Monitoring?

Your credit report is updated regularly to reflect credit activity changes. Credit monitoring allows you to have immediate visibility to changes in your credit report, providing you with the confidence that your credit identity is intact.

Equifax Complete™ Advantage Plan

As a consumer, you can take an active role in monitoring your personal credit information. Using Equifax's online tool, you can view your credit file 24/7 and monitor any changes, maintaining certainty that your credit score and identity have not been compromised.

For further information about Equifax Canada and protecting your identity, please visit www.equifax.ca. You can also visit the Financial Consumer Agency of Canada at www.fcac-acfc.gc.ca to learn more about credit reporting agencies.

Certain conditions apply to all offers. Equifax and EFX are registered trademarks of Equifax Canada Co. Inform Enrich Empower is a trademark of Equifax Inc., used here under license. ©2013 Equifax Canada Co. All rights reserved

ATB 2623 623

EQUIFAX

CONSUMER INFORMATION SOLUTIONS

Corporate Data Breach Solutions

What is a Credit Alert Flag?

How will a Credit File Alert Flag protect me from potential fraud activity?

A Credit File Alert Flag is one layer of identity theft protection. It provides peace of mind that your credit file has a warning system for credit lenders should anyone fraudulently try to seek credit in your name.

Equifax Canada Co. is Canada's largest credit reporting agency. A credit reporting agency is an independent organization that receives information from credit grantors and other (private and public) sources regarding individuals' credit activity. This information is compiled in a credit file for each Consumer.

Your credit file is a summary of your credit history. Your credit file contains information about your credit cards and loans, such as: when you opened your account, account balance, payment history, etc. Your credit file also includes personal information that is available in public records, such as a bankruptcy.

What is a Credit File Alert Flag?

A credit file alert flag is a narrative description that is placed on your credit file. This flag alerts credit grantors that the individual's personal identification may have been compromised. Credit grantors will then need to take further precautions to verify the identity of the person seeking credit. This may take the form of requiring the credit seeker to apply in person rather than over the phone or web, provide photo ID, or answer additional authentication questions. It is at the discretion of the lending institution's authentication protocol processes as to what steps they will take.

A Credit File Alert Flag stays on your credit file for a period of six years and it does **NOT** affect your credit score in any way. You have the option to choose to have it removed at any time within the six years by calling Equifax Canada at 1-800-465-7166.

For further information about Equifax Canada and protecting your identity, please visit www.equifax.ca. You can also visit the Financial Consumer Agency of Canada at www.fcac-acfc.gc.ca to learn more about credit reporting agencies.

Certain conditions apply to all offers. Equifax and EFX are registered trademarks of Equifax Canada Co. Inform Enrich Empower is a trademark of Equifax Inc., used here under license. ©2013 Equifax Canada Co. All rights reserved

APR 2023 623

DataPatrol™

A comprehensive 'early warning' service to protect data breach victims from the risks of identity theft and financial fraud combined with help and advice.

Experian℠

DataPatrol™

DataPatrol™ continuously monitors the web, social networks and stolen data sources to immediately detect and alert your customers should their personal and financial information be lost or stolen.

Someone to watch over your customers' data

Experian can help you deal with the consequences of a data breach providing your customers with a detection and support service that reduces the risks associated with data loss. Every year DataPatrol™ monitors over 20 million pieces of personal information that have been stolen and are traded online. It is the key to avoiding the disruption and financial losses which go hand in hand with identity theft and financial fraud. Sorting out the mess can take anything from 10 to 200 hours and in UK alone, it is estimated that cyber crime costs its victims over £3 billion per year*.

The identity theft experts at your service

Experian has a huge experience in addressing thousands of data breaches in a variety of sectors. With the latest addition of the award winning DataPatrol™ service, you can offer a trusted name in identity theft protection while addressing your customers' needs with a pro-active data monitoring service, customer alert and advice support.

Detection, alerting and support service

24/7 data monitoring

- Data monitored includes personal information such as name, usernames, passport number, driving licence; contact details such as email address, home address and phone number and financial details such as bank accounts and credit/debit cards.
- Immediate alert via email if any of the information on the user's DataPatrol™ account is detected within the monitored sources.
- Easy user interface, designed to prompt the users to be proactive if they are at risk of identity theft.

One click help and advice

- Dedicated customer service able to provide help and advice when customers receive an alert.
- Tips and advice on how to stay safe online and avoid becoming victims of identity and financial fraud.

*UK Cabinet Office Report: The Cost of Cyber Crime

АПВ 2023 623

Data Security Risk Management

nodatabreach.com provides risk management policies, procedures, training, and other tools to help insureds prevent a breach of confidential data.

As a Beazley Breach Response® policyholder, you have unlimited access to:

Legal compliance materials

Federal and state compliance materials regarding data security, data breaches, and data privacy, including:

- Summaries of federal & state laws
- Links to statutes & regulations
- Quick Tips on many subjects
- Sample forms, agreements, policies & procedures
- Continuing updates to the online content
- Electronic notification of significant changes

Monthly Newsletter, Tips & "Data Security Alerts"

Sent by email, learn about:

- Changes to laws & regulations
- Significant news & guidance regarding breaches and other privacy & data security issues
- Data security alerts provide timely notice of significant events that should not wait for the next monthly newsletter

Specialist support

Contact privacy specialists via toll-free hotline or email for help regarding:

- Privacy & data security compliance issues
- Data breach prevention issues
- Privacy & data security best practices

Step-by-step procedures to lower risk

Procedures and online forms to help you:

- Conduct a risk assessment
- Implement an incident response plan
- Test your incident response plan
- Understand and implement data security best practices

Training and awareness programs

- Online training courses with course completion records available via the system database
- Training bulletins for supervisors and staff—part of an ongoing training program
- Training posters to help raise privacy & data security awareness—part of an ongoing training program
- Webinars for compliance staff on current privacy & data security issues

Handling data breaches

Guidance provided to:

- Help prevent data security incidents
- Respond to a data breach



beazley

nodatabreach.com

Powered by ePlace Solutions, Inc.

ATB 8523 023

Beazley Group

Plantation Place South
60 Great Tower Street
London EC3R 5AD
United Kingdom

T +44 (0)20 7667 0623
F +44 (0)20 7674 7100

30 Batterson Park Road
Farmington
Connecticut, 06032
USA

T +1 (860) 677 3700
F +1 (860) 679 0247

Two Liberty Place
50 S. 16th Street, Suite 2700
Philadelphia
Pennsylvania, 19102
USA

T +1 (215) 446 8410
F +1 (215) 446 8469

Beazley Insurance Services
101 California Street
Suite 1850
San Francisco
California, 94111
USA
CA Lic. #0G55497

T +1 (415) 263 4040
F +1 (415) 263 4099

beazley

beazley.com/bbr

CBSL329_US_04/14

AFB 2623 623