peace of mind kit

At AccuPay, we take the trust you have placed in us very seriously. We understand that you depend on us to produce accurate payrolls as well as accurate tax returns and payments. With that in mind, we have created this "peace of mind" kit containing answers to common questions as well as information regarding AccuPay's bond and liability insurance. It is our hope that the information contained in this kit will ease your mind regarding any potential loss related to payroll.

FAQ's

Q: *Is AccuPay bonded?*

A: Yes, AccuPay is bonded, with coverage for errors and omissions as well as employee dishonesty (copy of certificate available upon request). AccuPay guarantees that your payrolls and tax payments will be accurate and timely, and will assume financial responsibility for errors and omissions which originated from any member of our staff. This includes tax penalties and/or interest due to late or inaccurate payments. In the event that the Client is responsible for the error or omission, AccuPay pledges to work on the Client's behalf to achieve the most desirable resolution.

Q: *Does AccuPay Outsource its Tax Pay Service?*

A: AccuPay uses a combination of expert, in-house staff and the advanced technology of MasterTax software to process client payroll tax payments and tax returns. AccuPay was spun off from a local CPA firm in 1994. Our staff consists primarily of Certified Payroll Professionals who are experts in payroll and payroll taxes. Our Tax Director is a CPA/CPP and our Tax Manager is certified in both payroll (CPP) and HR (SPHR). As such, we are very comfortable with collecting and filing payroll tax returns for our clients. Because of this, we can quickly and effectively resolve any tax issues that may arise.

Q: *Does AccuPay Have Bank References for its Financial Viability?*

A: Yes – AccuPay uses Regions Bank to originate its direct deposit and electronic tax transactions. AccuPay authorizes our prospective and current clients to inquire regarding AccuPay's financial condition and business reputation with our account representative, Melissa Zappata. Melissa may be reached at 317-221-6288.

Q: *Are AccuPay's Online Services Secure?*

A: AccuPay has licensed payroll software from Payroll Associates, Inc. since 2001. In that time, none of our clients have experienced a loss of any kind resulting from a breach in online security. In 2014, AccuPay licensed additional software from Kronos. Kronos applications reside in one of the only commercially available hosting environments that is compliant with Department of Defense (DoD) standards for a Sensitive Compartmented Information Facility (SCIF). Both production and offsite disaster recovery environments have completed SAS70 Type II audits and hold SafeHarbor certifications. (See attached for more information)

Q: *Does AccuPay have back-up servers and disaster recovery plans in place?*

A: AccuPay has implemented two back-up servers to allow continuous workflow in the event of a system failure of our Paychoice/Sage and Kronos software systems. In addition, AccuPay has installed a generator capable of powering AccuPay's entire facility and has implemented a back-up Internet connection to ensure continuous online capabilities.

AccuPay
Your Professional Payroll People

584 N. Emerson Ave, Greenwood, IN 46143
Phone: 317.885.7600 Fax: 317.885.7591
information@accupay.com

●●●● monitoring your EFTPS tax payments

You can monitor your Federal tax payments "24/7" by enrolling in the EFTPS system. Simply follow the detailed steps below to enroll in EFTPS.

1. Go to www.eftps.com
   (Note – you can also call EFTPS at 800-555-4477 and request an enrollment form)
2. Click on the "Enrollment" tab at the bottom right in red
3. Read the privacy act disclosure and click "accept"
4. Enroll as a "business" and then click "next"
5. Enter your business information, contact information, financial information (Select the second option), "payment through a financial institution", and click "review"
6. Verify the accuracy of your enrollment information, read the authorization agreement and complete the electronic signature with the contact person's name, and enter the company's Federal EIN
7. Click/Check "accept" on the disclaimer and click "complete"
8. You will see an acceptance screen from EFTPS that provides you with an enrollment trace number. Print this screen for your records.

EFTPS will send you an enrollment packet with your PIN and log-in information. Once the packet arrives, proceed as follows:

1. Call the EFTPS at their toll-free number and follow the instructions to receive your temporary password.
2. Log on to the EFTPS and change your password
3. After obtaining confirmation, navigate to the "Payments" tab on the EFTPS website anytime to review a history of your Form 941 payroll tax deposits
4. **"Match"the EFTPS payment history with tax deposit information provided to you by your payroll company. AccuPay's "Tax Liability" report has a "Total Federal Tax" amount and date you can match to.**

AccuPay
Your Professional Payroll People

584 N. Emerson Ave. • Greenwood, IN 46143 • 317.885.7600 • Fax: 317.885.7591 • payroll@accupay.com

The Hanover Insurance Group

Hanover Professionals

DECLARATIONS ***Advantage Portfolio***

THIS IS A CLAIMS-MADE POLICY. PLEASE READ THE POLICY CAREFULLY.

MISCELLANEOUS PROFESSIONAL LIABILITY POLICY

Policy Number	Coverage is provided by:	Agency	Agency Code
LHW 9909230 04	The Hanover Insurance Company 440 Lincoln Street Worcester, MA 01653	JACKSON-MCCORMICK INS	6604516

Issue Date: 03/03/2017

Item 1. Named Insured and Address:
ACCUPAY INC
584 N EMERSON AVE
GREENWOOD, IN 46143

Item 2. Policy Period:
Inception Date: 04/09/2017
Expiration Date: 04/09/2018
12:01 A.M. Standard Time at the address of the Named Insured as stated herein

Item 3. LIMIT OF LIABILITY
Limit of Liability
a. $100,000 for each **Claim**; not to exceed
b. $300,000 for all **Claims** in the aggregate

Item 4. DEDUCTIBLE: $5,000 Each Claim

Item 5. RETROACTIVE DATE: 04/09/2013

Item 6. PROFESSIONAL SERVICES

Payroll Processing

Item 7. PREMIUM FOR THE POLICY PERIOD:

Total Premium: $1,444.00

Item 8. NOTICE OF A CLAIM
Report any claim to the Company as required by Section **G. DUTIES IN THE EVENT OF CLAIM(S) OR POTENTIAL CLAIM(S)**:

The Hanover Insurance Company
P.O. Box 15145
Worcester, MA 01615

National Claims Telephone Number: 800-628-0250
Facsimile: 800-399-4734
Email: firstreport@hanover.com

Item 9. Forms attached at issue:

910-0002	01/12	Miscellaneous Professional Liability Policy - Declarations
910-0001	12/09	Miscellaneous Professional Liability Insurance Policy
231-0862	12/14	Customer Notice of Privacy Policy and Producer Compensation Practices Disclosures Privacy Policy Disclosure
401-1268	08/12	U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") Advisory Notice to Policyholders
401-1281	01/13	Notice To Indiana PolicyHolders Regarding Filing Complaints with the Department of Insurance

910-0140	10/11	Notice to Policyholders: Information Regarding Extended Reporting Period ("ERP Coverage")
910-0078	01/12	Privacy Provisions of HIPAA Carve-Back Endorsement
910-0086	01/12	Tax Preparers Endorsement
910-0113	11/09	Indiana Miscellaneous Professional Liability Amendatory Endorsement
910-0183	01/12	Exclusion - Management Consultants
SIG-1100	08/16	Signature Page

Item 10. Producer Name and Address: JACKSON-MCCORMICK INS
P.O. BOX 523
LEBANON, IN 46052

TRAVELERS

Wrap+®

CRIME
DECLARATIONS

POLICY NO. **105753263**

Travelers Casualty and Surety Company of America
Hartford, Connecticut
(A Stock Insurance Company, herein called the Company)

ITEM 1	**NAMED INSURED:** **ACCUPAY, INC.** D/B/A: Principal Address: **584 N. EMERSON AVENUE** **GREENWOOD, IN 46143**
ITEM 2	**POLICY PERIOD:** Inception Date: **February 28, 2015** Expiration Date: **February 28, 2018** 12:01 A.M. standard time both dates at the Principal Address stated in ITEM 1.
ITEM 3	**ALL NOTICES OF CLAIM OR LOSS MUST BE SENT TO THE COMPANY BY EMAIL, FACSIMILE, OR MAIL AS SET FORTH BELOW:** **Email:BSIclaims@travelers.com** **FAX:(888) 460-6622** **Mail:Travelers Bond & Specialty Insurance Claim** **385 Washington St. – Mail Code 9275-NB03F** **St Paul, MN 55102**
ITEM 4	**COVERAGE INCLUDED AS OF THE INCEPTION DATE IN ITEM 2:** Crime

©2009 The Travelers Companies, Inc. All Rights Reserved

ITEM 5

CRIME		
Insuring Agreement	**Single Loss Limit of Insurance**	**Single Loss Retention**
A. Fidelity		
1. Employee Theft	**$500,000**	**$5,000**
2. ERISA Fidelity	**$500,000**	**$0**
3. Employee Theft of Client Property	**Not Covered**	
B. Forgery or Alteration	**$100,000**	**$1,000**
C. On Premises	**Not Covered**	
D. In Transit	**Not Covered**	
E. Money Orders and Counterfeit Money	**Not Covered**	
F. Computer Crime		
1. Computer Fraud	**Not Covered**	
2. Computer Program and Electronic Data Restoration Expense	**Not Covered**	
G. Funds Transfer Fraud	**Not Covered**	
H. Personal Accounts Protection		
1. Personal Accounts Forgery or Alteration	**Not Covered**	
2. Identity Fraud Expense Reimbursement	**$25,000**	**$0**
I. Claim Expense	**$5,000**	**$0**

©2009 The Travelers Companies, Inc. All Rights Reserved

Data security and compliance were top of mind when developing Kronos' infrastructure. To ensure that Kronos remains an industry leader in delivering SaaS, recurring audits and certifications are completed. Examples include:

- SSAE 16 - is an enhancement to the SAS70, which spells out how an external auditor should assess the internal controls of an outsourcing service provider and issue an attestation report to outside parties or to a client.
- Safe Harbor - prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection.

Data Centers

Our data and your data, is hosted in both a primary data center, in addition to disaster recovery facilities, which ensures both the physical security of the data and a consistent uptime for the applications. Our data centers also undergo several certifications and complete a number of rigorous audits to ensure compliance and safeguarding of data.

Our primary server farm resides in one of the only commercially available data centers compliant to the Department of Defense (DoD) standards for a Sensitive Compartmented Information Facility (SCIF).

Security

Surrounded by an iron fence, the facility perimeter is equipped with pan-tilt-zoom (PTZ) surveillance cameras and a 24-hour guard station to monitor access. Only pre-approved visitors are granted access during normal business hours and may only access common meeting space. All parking for visitors is restricted to areas outside the fenced perimeter and employee access to the data center requires biometric identification.

All power and data lines are encased in armored conduit. Specially designed Lampertz vaults protect servers, network cabling, power sources, and related hardware against fire, smoke, water, moisture, and electromagnetic pulses. Vault doors are secured with biometric thumbprint readers and monitored by security cameras. Added security is achieved through a multiple-layer intrusion detection system consisting of custom firewall rule sets, private VLANs, and two layers of isolation.

Reliability

The facility is designed so there is no single point of architecture failure. System operation is monitored 24x7x365 and includes N + N power redundancy, connectivity to multiple backbone providers, and variable switch load balancing. All new servers have hardened operating systems and are given vulnerability scans.

To ensure maximum uptime, the HVAC system maintains a consistent operating temperature and is powered by multiple 20-ton computer-room air conditioning units and three 100-ton chillers. Redundant power lines provide over 265 watts of power per square foot utilizing 2-megawatt transformers. In the event of a power outage, a 2-megawatt Caterpillar diesel generator provides full load in less than 10 seconds and can run for more than 24 hours without refueling. In the event of an emergency, time-guaranteed contracts with multiple diesel suppliers ensure uninterrupted service.

PayChoice Security and Business Continuity Overview

PayChoice operates within the following operational guidelines:

Hosting:

PayChoice systems operate within secure cages at two co-location facilities - one operated by Switch & Data, (www.switchanddata.com) and one operated by DBSi, (www.dbsintl.com). Secure access is monitored 24 hours a day and all entry to the facility is logged. Access is restricted to authorized individuals only.

Backup:

Business-critical data is backed up nightly to disk or to robotic tape library. Media is periodically restored to test data integrity and validity of the backup.

Security:

Application tiers are configured according to commercially accepted practices. The customer facing web tier operates behind Cisco firewalls in a DMZ environment. Application and data tiers operate in a secure non-visible area of the network.

Applications require authentication for all types of users. Data is stored and transmitted securely using 128-bit encryption.

Secureworks (www.secureworks.com) provides managed security services, including firewall management and monitoring, Intrusion Prevention Systems /Intrusion Detection Systems (IPS/IDS) management and monitoring, log analysis, and vulnerability testing.

Centrally monitored endpoint protection is in place to prevent rogue applications, viruses, worms and other malware from infecting the infrastructure.

Business Continuity:

The PayChoice Business Continuity strategy addresses both component level outages and facility level outages. In the event of a component failure, a new component will be utilized to restore service. If the failed component was a server, the appropriate data would be restored from backup. In the event of a facility outage, work would be shifted to other PayChoice processing centers. The PayChoice Disaster Recovery (DR) site is located in the Moorestown, NJ Headquarters facility. This site can support operations in the event of an outage at our other data centers.

The co-location facilities itself provides redundant power and Ethernet hand-off to the PayChoice infrastructure. Power is backed up by generators with capacity to run the entire facility including cooling. Backup power and cooling infrastructure is tested on weekly and monthly intervals.

Our Commitment

AccuPay is committed to protecting the personal information of you and your employees.

Below are some tips that will help us keep your information protected:

Never email social security numbers of your employees or any other sensitive information.

Please assign a specific contact person(s) with whom AccuPay may discuss your payroll information.

Please notify your employees that AccuPay is unable to disclose any payroll information to them without prior approval from the above mentioned contact(s)

AccuPay
Your Professional Payroll People

584 N Emerson Ave
Greenwood, IN 46143

Phone: 317-885-7600
Fax: 317-885-7591
E-mail: payroll@accupay.com
www.accupay.com

privacy policy

AccuPay
Your Professional Payroll People

How AccuPay protects and uses client information

At AccuPay, we believe that protecting your privacy is an integral part of the customer service we provide to you. This disclosure describes how we use and protect information provided by our clients in connection with payroll processing, tax payment services, and accounting.

- We do not sell customer information to third parties.
- We do not share customer information with outside parties who may wish to market their products to you.
- AccuPay's employees safeguard your customer information carefully through internal controls and procedures.

We collect and maintain customer information as part of servicing your account and your customer relationship.
In the course of serving you, we collect information about you, your employees, and your business primarily from information you provide to us on forms or via phone, fax, or email.

The information we collect is used to process your payroll and (if applicable) pay your payroll taxes in compliance with all laws and regulations governing such actions. Information may be used by AccuPay as well as with authorized third parties for a number of purposes, such as:

- ✓ **To service your accounts** by processing ACH transactions (direct deposits), tax payments, payroll, W-2's, 1099's or accounting services.
- ✓ **To keep you informed of the rules, regulations, and laws pertaining to payroll, HR, and business accounting through our PayDay emails.**
- ✓ **To provide personalized promotional offers.**

We do not share customer Information with outside parties who may wish to market their products to you.
We may disclose the information we collect, as described above, with nonaffiliated third parties that are acting on our behalf, or as permitted by law, including:

- ✓ Companies that perform support services for us, such as data processors, technical systems consultants and programmers, retirement or insurance providers, or Worker's Comp insurance providers.
- ✓ Government entities, courts or other entities (in response to subpoenas and other legal processes), or those with whom you have requested us to share information.

Important contact information for current customers.
As a customer, please note that if you choose not to receive communication by email, you may continue to receive marketing information from AccuPay in regular payroll packages, as part of your online payroll reports, or when you visit us online. You may also receive survey or customer care calls. If you do not wish to receive these calls, please contact AccuPay in writing. Requests may be sent to:

AccuPay, Inc.
584 N. Emerson Ave
Greenwood, IN 46143

Or be sent via email to :
payroll@accupay.com

The policies and practices described in this disclosure are subject to change, but we will communicate any significant changes to you.