



**PARTNER  
COUNCIL**

A HAWK INCENTIVES EVENT



# Blackhawk Network's Compliance & Risk Program



September 12, 2018

Mabel Wilson, VP, Regulatory Compliance, Blackhawk Network  
Stephanie O'Brien, Principal Legal Counsel, Blackhawk Network

# Information Sharing Today






---

- Why we do what we do for regulatory compliance and fraud risk management
- The cost of non-compliance
- Best practices for operational effectiveness and fraud mitigation
- Legal and government relations support



# Regulatory Compliance & Fraud Risk Management

# Regulatory Drivers for Blackhawk's Prepaid Program

Attributes of our Business Model	Regulatory Implications
 <p>We are US-based company.</p>	<ul style="list-style-type: none"><li>• Various US regulations</li><li>• US OFAC &amp; sanctions</li></ul>
 <p>We conduct business in many countries.</p>	<ul style="list-style-type: none"><li>• Anti-corruption laws</li><li>• Department of Justice oversight</li><li>• International sanctions</li></ul>
 <p>We are defined as a “money services business.”</p>	<ul style="list-style-type: none"><li>• State money transmission laws</li><li>• International licensing</li><li>• Anti-money laundering</li><li>• Issuing bank requirements</li></ul>
 <p>We collect personally identifiable information from employees, corporate clients, and consumers.</p>	<ul style="list-style-type: none"><li>• Privacy laws</li><li>• Data breach disclosure laws</li><li>• Asset protection</li></ul>
 <p>We market directly to consumers and use agents and resellers.</p>	<ul style="list-style-type: none"><li>• Consumer protection laws</li><li>• Consumer marketing materials</li><li>• Clear contractual terms</li></ul>

# How Compliance Supports Prepaid Programs

---

- Understand and analyze applicable laws for implementation
- Pay attention to and achieve relevant industry certifications
- Employ efficient and effective risk management and fraud prevention processes
- Train our employees and third party representatives
- Engage our partners in open and ongoing training and communication
- Configure our systems to automatically limit exposure to money-laundering, cyber, and other risks
- Conduct transaction monitoring to identify unusual activity

# Demonstrated Through:



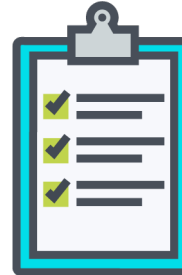
## Security

Annual PCI DSS assessment  
Onsite Cyber Defense Center  
Visa and Mastercard certified card production and fulfilment facilities\*  
ISO 27001 certification underway



## Anti-Money Laundering & Financial Regulations

State money transmission licenses in all required jurisdictions  
Anti-Money Laundering Risk Management Program  
Global sanctions reviews  
Regulatory change management  
24x7 fraud support



## Corporate Compliance

Risk & Governance Committees  
SOX certification  
Anti-Corruption Program  
Third-Party Risk Management Program  
Employee background checks  
Formal employee training program



## Prepaid and Payment Network

SSAE 16 SOC 1 Type 2 Report  
24x7 Network Operations Center  
Formal change control process  
Business Continuity & Disaster Recovery Program



## Consumer Protection & Privacy

TRUSTe-certified for key consumer websites  
Global Privacy Program based on FTC FIPPs & Privacy Shield  
Consumer Protection Program

*\*Owned and operated by third-party service providers*

# The Cost of Non-Compliance



# Disregard for Sanctions: PayPal

---

\$7.7M

The US Treasury Department (OFAC) fined PayPal for violating US economic sanctions requirements when employees failed to comply with company policies

Base penalty amount was **\$17 million**  
for 136 transactions for ~\$7,000 or ~\$50/transaction

# Anti-Money Laundering: Western Union

---

\$586M

Western Union forfeits in settlement with FinCEN, DOJ, FTC and certain US states after admitting to criminally violating the BSA and Federal AML regulations

“... Reflects ... the damage that can be done when there is a failure of a **culture of compliance.**” — FinCEN Acting Director Jamal El-Hindi

# Consumer Protection: UniRush & Mastercard

—  
\$13M

The Consumer Financial Protection Bureau (CFPB) ordered UniRush & Mastercard to pay for UDAAP and violation of federal consumer protection laws.

The CFPB received about **830 consumer complaints** in weeks; cf. 147 from Nov 2014 to Jan 2015. \$10 million for consumer restitution, \$3 million civil penalty

# Consumer Protection: Netspend

—  
**\$53M**

Netspend settles with the Federal Trade Commission (FTC) for deceptive consumer marketing practices of prepaid card sales.

Company barred from further misrepresentations.  
**\$40 million** to customers, **\$13 million** to the FTC

# State Enforcement Actions

---



**\$60M**

New York fines Western Union for AML violations



**\$507K**

Florida fines Square for engaging in money transmission activities without a license



**\$83K**

Texas fines AvidXchange for engaging in money transmission activities without a license

# Trends in Regulatory Prosecutions

---

- Multi-jurisdictional, multi-agency prosecution
- Retroactive prosecution, several cases go way back
- Targets come in all sizes
- Technology enhances access and ability to analyze massive amounts of data
- Increased focus on Board/executive oversight and culture of compliance and ethics
- Huge fines and penalties for corporations
- Loss of employment, personal financial liability and prison time for individuals

# Operational Effectiveness & Fraud Mitigation



# Regulatory Support for Resellers

---

- Use of Blackhawk's U.S. State money transmission licenses ("MTLs")
- Reseller operations manuals includes guidance and AML training
  - **For Business Funded U.S. Dollar Products:**  
<http://bhnpartnerships.com/wpdm-package/partner-operations-manual-u-s/>
  - **For Business Funded Canadian Dollar Products:**  
<http://bhnpartnerships.com/wpdm-package/partner-operations-manual-canada/>
  - **For Consumer Funded U.S. Dollar Products:** <https://connect.blackhawknetwork.com/publically-accessible-reference-documents/bhn-ecommerce-distribution-partner-operations-manual>
- Defined product catalogs for business funded and consumer funded
- Customer Due Diligence (CDD) reviews on reseller's end client
- Enhanced CDD performed to fulfill "Fifth Pillar" requirements
- Sanction reviews using U.S. and international lists
- Bulk order level monitoring reduces keying errors and fraud
- Transaction monitoring for unusual cardholder activity with BHN submitting Suspicious Activity Reports (SARs)



# Fraud Trends: How to Mitigate Your Losses

---

- **Prepaid Product Fraud:** Blackhawk assumes negative balance losses and true cardholder fraud
- **Unusual Payments:** Verify the payment comes from your client
- **Payment Fraud:** Make sure your client's payment "clears", prior to placing your client's order
- **Fraudulent Credit Card Payments:** Compare your client's ship to address to your client's credit card billing address
- **Virtual Product Fraud:** Batch delivery of virtual product is redeemed immediately; payment to reseller does not "clear"
- **Internal Embezzlement:** Use the "two-man rule"; Limit ordering to a specific employee(s); Ship product to another specific employee(s)
- **Refund Payment Fraud:** Send client refunds back to the original payment source or location

# Best Practices for Resellers

---

- Know Your Client — #1 fraud and money laundering preventer
- Read and understand the Blackhawk reseller operations manuals
- Know the regulations that apply to the resale of prepaid access products
- Retain records of your client's information, your client's payments and be sure to protect the demographic data your clients provide
- Train your employees using the Blackhawk reseller operations manuals
- Pay attention to and act on unusual activity and fraud trends
- If you have any concern contact Blackhawk immediately!
  - **Regulatory compliance assistance:** Ryan Schmitz (Director, Regulatory Compliance) at 636.226.2089 or [ryan.schmitz@bhnetwork.com](mailto:ryan.schmitz@bhnetwork.com) or [Fenton.ComplianceQuestions@bhnetwork.com](mailto:Fenton.ComplianceQuestions@bhnetwork.com)
  - **Fraud reporting:** Email [investigations@bhnetwork.com](mailto:investigations@bhnetwork.com)
  - **All other assistance:** Contact your Blackhawk Account Manager

# Legal & Government Relations Support



# Contract Overview

---

## Flow down of compliance obligations and regulatory requirements:

### ***e. Information Requests:***

BES, the Issuer, and the Network may require Client to provide certain information to identify: (i) the intended use of Cards issued under this SOW, (ii) Client's identity, and (iii) Client's owners. Such information may be used to comply with applicable anti-money laundering laws, and to confirm that the Cardholder Agreement will comply with applicable laws, rules, and regulations. Based upon the information so provided (or Client's failure to provide such information), BES, the Issuer, and the Network reserve the right to withdraw approval for Client's program.

### ***g. Terms Applicable to Open Loop Prepaid Cards:***

**i. General:** Open Loop Prepaid Cards may be anonymous or personalized, as identified in this SOW. For personalized Open Loop Prepaid Cards, Client shall provide only the first name and last name, or first initial and last name, of a natural person. If Client provides any text or symbols to BES other than the first initial or name and last name of the natural person Participant, (i) Client shall assume any and all costs and liabilities incurred as a result of such action, (ii) the Card shall be treated as an anonymous card for customer service purposes. As applicable, the personalized Card demographic data must include Participant's home address regardless of the shipment method. Client shall transmit Participant home address and updates thereto as necessary to BES regardless of the shipment method specific to personalized Cards. Should addresses other than the Participant's home address be provided, Client accepts and acknowledges that the Card may be suspended and/or cancelled and the Card may not function at the point of sale. BES reserves the right to deny participation or cancel any issued Open Look Prepaid Card for any Participant or proposed Participant should the name of the Participant appear on the Office of Foreign Assets Control ("OFAC"), Office of the Superintendent of Financial Institutions ("OSFI") or Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") lists, or other local, state, federal, or foreign lists of individuals being pursued by law enforcement agencies, or other such legal or risk related reasons as solely determined by BES.

# Legislative/Regulatory Monitoring & Government Relations

---

- Membership in industry trade groups (NBPCA, Card Coalition)
- Retain government relations experts in DC
- Participation in special interest groups and task forces
- Proactive outreach to educate legislators and regulators and their staff

# Regulatory Guidance: Ensuring Regulation Matches Industry

---



CARD Act and  
implementing regulations:  
“loyalty, award, promotional”  
exclusion



Prepaid Accounts Rule:  
narrowing scope

# Legislative Activity: Examples

---



Directly address  
troublesome legislation  
(Illinois: rebate bill)



Amend language to minimize  
unintended scope/impact  
(Hawaii: virtual currency;  
Arizona: “gift cards”)



Sponsoring legislation to clarify  
regulatory effects  
(North Carolina: MTL)



Thank You