

---

# ***Account Takeover Fact Sheet***

## Detecting unauthorized use of online access credentials

### **Advisory services**

#### Forensic services

### **Account takeover fraud assessment**

Organizations which provide online account access for customers are facing increased cyber fraud loss involving “account takeover,” i.e. the unauthorized use of login credentials. Once the account is accessed, the unauthorized user can view a variety of protected data sets including PII, PCI, PHI, and student records depending on the type of account and the organization. Further, with Financial Services organizations, many online accounts permit the movement of currency once the account has been accessed.

Based on our incident response engagements helping clients forensically investigate these fraud incidents, we have found the typical risks to include:

#### **Phished customers**

Highest probability: This attack does not always result in theft of all authentication elements required to login and thus requires the criminal to perform logic reconnaissance on the Web application.

#### **Phished insiders**

High probability: Insiders with access to customer information also have access to the Internet and sometimes unintentionally open a malicious email attachment or link. Criminals can easily spam the entire address space of an organization or target specific users, known as spear phishing. Social networks have made intelligence gathering for targeting insiders much easier.

#### **Cyber attack – network intrusion**

Medium probability: A criminal enterprise “hacks” external-facing web servers, etc. and then enumerates the network to find the storage locations of the data of interest or simply collect network traffic using malicious “sniffers.”

#### **Insider**

Low probability: An insider with access to customer data uses it to commit the fraud or sells the information to criminals who commit the fraud. Inter-personal conflict, work disenchantment, and financial distress are leading influences of the insider threat.

Understanding the root cause, scope of the defrauded accounts, and quantification of impacted customers is a complex effort in crisis mode when the organizational risks are high: Privacy breach notification, legal actions by victimized customers, public embarrassment and reputational damage, etc. Based on PwC's past incident response performances involving this type of fraud, we have developed a proactive fraud assessment.

### **“Account takeover” fraud assessment**

How can an organization determine if online customer accounts are being used by unauthorized individuals or criminal enterprises? Using real lessons learned from the forensic investigation of such cyber fraud in a reactive capacity for our clients, PwC offers an innovative fraud assessment which is designed to analyze the cyber behaviors of online customers.

---

# *Account Takeover Fact Sheet*

## Detecting unauthorized use of online access credentials

### Advisory services

#### Forensic services

### Account takeover fraud assessment Prep

PwC provides the client with a list of data elements needed to assess customer online behavior. This data is contained in a variety of system logs. Once gathered PwC will forensically collect the data and transport it to our forensic lab. We do it forensically to help our clients in the event of a future legal or regulatory proceeding. The client will identify which customer accounts are within the scope of the assessment.

### Cyber behavior analysis

Leveraging the log data provided by the client, PwC will ingest that data into its propriety OBAT (Online Behavioral Analysis Tool) which was developed during PwC cyber fraud incident response engagements. PwC professionals will customize OBAT to accommodate the specific log data provided which is often unique to any given client's IT environment. PwC professionals will use OBAT to profile cyber behaviors associated with the customer accounts within scope. The objective is to identify the normal account access behaviors in order to expose suspicious account accesses.

### Discover currently unknown fraudulent activity involving online customer accounts

PwC's fraud assessment helps our clients understand normal online behavior for any given customer. By doing so, suspicious online behavior can be detected. Previously unknown account accesses could be identified and further cyber fraud loss prevented.

PwC's fraud assessment can be leveraged as a 1-time assessment, a series of rolling assessments against new and different accounts, or as an ongoing component of your cyber fraud detection program. Further, the assessments could be conducted under the privilege of a "legal risk assessment" through legal counsel in an effort to protect the findings from any future legal or regulatory proceedings.

For more information, please contact

**Dave Burg**

703 918 1067 | david.b.burg@us.pwc.com

---

**Shane Sims**

703 918 6219 | shane.sims@us.pwc.com

---

**Ed Gibson**

703 918 3550 | ed.gibson@us.pwc.com

---

**Kimberly Peretti**

703 918 1500 | kimberly.k.peretti@us.pwc.com

---

**David Nardoni**

213 356 6308 | david.nardoni@us.pwc.com

---

**Tomas Castrejon**

415 498 8418 | tomas.m.castrejon@us.pwc.com

---